EXTRACT FROM DATA PROTECTION CODE OF PRACTICE

8. DATA SHARING

Introduction

The University collects a wide range of personal data relating to staff and students for the University's purposes and to meet its external obligations. Both these types of data collection may result in the eventual transfer of personal data to third parties, which the University must ensure is permitted under the DPA 1998.

8.1 Conditions for Processing of Personal Data

In order for the University as a data controller to lawfully process personal data one of the following conditions must be met:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract with the individual
- Processing is required under a legal obligation (other than a contractual one)
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions, e.g. administration of justice, or for exercising statutory, governmental, or other public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties and is not unfair to the individual

8.2 Conditions for Processing of Sensitive Personal Data

Where sensitive personal data is concerned one of the ordinary processing conditions at 8.1 above and one of the conditions for processing sensitive data below must be met before processing can be carried out. The conditions for processing sensitive data are:
the data subject has given his or her explicit consent to the processing of the personal data; or that the processing is necessary for a further set of specified reasons, including:

- It is required by law for employment purposes
- It is needed in order to protect the vital interests of the individual or another person
- It is needed in connection with the administration of justice or legal proceedings

8.3 Key Elements

The following requirements must be adhered to when considering the sharing of personal data:

- **Purpose** - there should be a clear and lawful purpose for the data sharing.
- **Fairness** - the nature and extent of the data sharing should be a proportionate means of achieving that purpose when weighed against the interests of the individuals concerned e.g. consider whether the data could be anonymised.

- **Transparency** - the data subjects should be given appropriate notice in advance about the possible sharing of their personal data. Failure to do so may mean that it is considered to have been carried out unfairly and without due respect for the data subjects' rights

The data subjects must be able to effectively exercise their rights under the DPA 1998 including the rights to access data which is held about them and to object to, or opt out of, certain types of processing. While transfers will be permitted where data subjects have given their consent to the transfer, a positive response must be received and consent cannot be inferred from silence.

8.4 Data Sharing within the University

There are two common misconceptions about sharing personal data within the University. The first is the assumption that because personal data is held by one department it can be shared automatically with other departments or University employees because "we all work for Edinburgh Napier University". The second is the converse i.e. that personal data cannot be shared with other departments or colleagues. Where there are no restrictions on the sharing of personal data under either the DPA 1998 or other legislation, e.g. the Equality Act 2010, personal data may be shared on a strictly "need to know" basis having first considered the purpose, fairness and transparency of such a sharing.

8.4.1 Sensitive personal data

The University has stringent requirements in place for the transfers of sensitive personal data , which are dealt with in Section 12 of this Code of Practice. The advice of Governance Services, the Head of Disability and Inclusion or the University's Diversity Partner should be sought if in any doubt.

8.5 Data Sharing with Third Parties

8.5.1 The two main types of data sharing are:

a) a systematic, routine data sharing where the same data sets are shared with the same third party agency or organisation for an established purpose or;

b) an exceptional, one-off decision to share data for any of a range of purposes.

There are two contexts in which the University will share personal data with third party agencies and organisations:

i) where we are required to do so by law; and

ii) where it is necessary for us to do so within the context of general operations and primarily for the provision or administration of educational services.

In the case of i) above a list of the third parties to whom such disclosures are required can be consulted.

In all situations where ii) above applies the three requirements of **purpose**, **fairness** and **transparency** must be met before any data sharing with third parties takes place.

8.5.2 The University must ensure that personal data under its control is not disclosed or transferred to unauthorised third parties. These will include a person or organisation:

- not covered by the data processing conditions relied upon by the University, referred to at 8.1 and 8.2 above, unless the DPA 1998 expressly permits such disclosure or transfer.
- covered by the data processing conditions relied upon by the University under 8.1 and 8.2 above, but where the request is for reasons outside the scope of those conditions, unless the DPA 1998 expressly permits such transfers without such consent.
- not disclosed in the University's fair processing statements for students and staff as a likely recipient or class of recipient of their data, unless the DPA 1998 expressly permits such disclosure or transfer.

"Unauthorised third parties" may include family members, friends, local authorities and government bodies unless disclosure is permitted under the Act or required by other legislation.

8.5.3 Any member of University staff who is considering a data sharing arrangement should consult and then complete the checklist of the relevant issues **before** any data sharing takes place.

8.5.4 Where it is decided that a data sharing arrangement is to be made, an appropriate agreement **must** be put in place **before** any data is transferred. The type of agreement used will depend on which of two forms of data sharing is proposed i.e. either i) by the University as a data controller with a third party who is also a data controller i.e. both parties determine the purposes for which and the manner in which the personal data is to be processed; or ii) by the University as a data controller with a third party who will then process that data on the University's behalf i.e. as a data processor.

8.5.5 If ii) above applies the University must ensure that in all such cases, the agreement must expressly require that the data processor:

- will act only on instructions from the data controller; and
- has security in place that is equivalent to that imposed on the University by the seventh data protection principle

A data processor does not therefore have any direct data protection responsibilities of its own. As these are all imposed on the data processor through its agreement with the University, the University has a duty to ensure that the data processor carries out the terms of the agreement by monitoring its compliance.

Guidance on the forms of data sharing and the template agreements or clauses to be used for 8.5.4 i) and ii) above should be sought from Governance Services **before** any data sharing takes place.

8.6 Handling requests for Personal Data: disclosures without consent

8.6.1 The University will handle requests for disclosure of personal data as follows:

i) Requests made by the police or authorities with prosecuting powers will be dealt with under the DPA 1998;
ii) All other third parties requests, including e.g. those referred to in 8.10 and 8.11 below, will be treated as requests under the Freedom of Information (Scotland) Act 2002 (FOISA).

University staff who receive a request from a third party should seek advice as necessary from Governance Services.

8.6.2 Under the DPA 1998, data may be disclosed to third parties without consent **only** where the Act expressly permits such transfers e.g. where it is required for the purposes of:

i. Protecting the vital interests of the data subject (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject)
ii. Preventing serious harm to a third party that would occur if the data were not disclosed
iii. Safeguarding national security
iv. Prevention or detection of crime
v. Apprehension or prosecution of offenders
vi. Assessment or collection of any tax or duty or of any imposition of a similar nature
vii. Discharge of regulatory functions, including securing the health, safety and welfare of persons at work

With regard to iv. to vii. above it should be noted that disclosure is allowed in those cases **only** to the extent to which failure to disclose would be likely to prejudice the attainment of those aims. This means that if the information was not disclosed this would noticeably damage those purposes.

8.6.3 Where the police or authorities with prosecuting powers are seeking the disclosure of personal data for the purposes referred to in 8.6.2 iii. – vii. above, the University will normally require that they submit their respective organisational form to an authorised officer in Governance Services. The UK Information Commissioner's guidance on Releasing Information to Prevent or Detect Crime will be applied in determining whether a disclosure is permitted.

8.6.4 All external third parties requesting personal data under FOISA will normally be required to submit their request in a letter on headed notepaper, addressed to an authorised member of University staff. The request will then be considered as set out in 8.10 i) and ii) below.

8.6.5 All third parties should give:

- the authority under which the request is made

- reasonable proof of the requester's personal identity and organisational affiliation e.g. police officers will be expected to quote their identification numbers and/or produce their warrant cards
- details of the nature of the personal data and the purpose for which it is being requested and confirmation that the scope of the request is necessary and proportionate
- where applicable, the relevant exemption under the DPA 1998 or other legislation which authorises the University to release the information
- where applicable, a warranty that it will be held and processed in conformity with the Data Protection Principles

The absence of such documentation or a warrant may be justification for refusal to disclose the requested personal data.

Once the request has been received, relevant staff should consult and then complete the checklist at 8.5.3 above for such one-off requests for personal data.

8.6.6 Alternatives may be for staff to accept a sealed envelope which they will attempt to forward to a student's last-recorded address or to forward an incoming email message to a student **without** confirming the student's attendance at the University.

8.6.7 In appropriate circumstances and where the matter is urgent, an attempt should be made to contact the subject by phone, or other means, in order to provide them with information about the enquirer and the nature of the enquiry, so that they can choose whether to respond

8.6.8 Disclosures without consent may be made normally only by an authorised officer in Governance Services or other authorised member of University staff, in consultation with Governance Services. Records of disclosures made by Governance Services under 8.6.3 will be maintained centrally and those under 8.6.4 will be kept by the relevant authorised University staff.

8.7 Emergency Requests

An emergency situation is one where there is reason to believe that there is a danger of death or injury to the data subject or any other person. In such situations, University staff receiving a request are required:

- To seek the authorisation of their Dean of School or Service area or nominated deputy before disclosure
- Not to disclose data where they have doubts as to the validity of the request
- Where the request is received by telephone, to ask the caller to provide a switchboard number and call them back through the organisation's switchboard before providing the data
- To make a record of the enquiry as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place and pass this to Governance Services.
- To ask the enquirer to follow up their request with a formal written and signed request, so that this may also be passed to Governance Services to retain centrally

Provided **only** that there is time to do so and no delay would be caused to a data sharing which is deemed necessary in an emergency, the relevant member of staff should consider consulting the checklist at 8.5.1 above for such a “one-off” request.

8.8 Mandatory Disclosures

The University may be required by legislation, by any rule of law or by the order of a court to disclose an individual's personal data. A non-exhaustive list is available of Third Parties Who May Require Disclosure

With the exception of a court order, the request should be made on headed notepaper, ideally cite the relevant exemption and be signed by an authorised officer. The data disclosed should be the minimum required to accede to the request, it must be sent by or provided in the most appropriate secure method and a record of both the request and the data disclosed must be kept.

8.8.1 Court orders

The University has a legal obligation to respond to valid Court orders promptly and with the information requested, regardless of whether this is sought for the pursuer or the defendant. Court Orders should be marked “confidential and urgent” and passed immediately to the following University staff who will be responsible for ensuring that the information is collected and sent timeously by the most appropriately secure method:

For students/former students: Director of Student & Academic Services or nominated Assistant Director

For Staff/former staff: Director, Human Resources or his/her nominee

Guidance may be sought from Governance Services or other authorised staff in Governance Services.

8.9 Disclosures to Employees under Discrimination Legislation

The nature of the disclosures required by the University as an employer under e.g. the Equality Act 2010 will raise data protection issues for employees other than the employee making the enquiry. Advice and guidance must be sought from the Director of Human Resources or his/her Depute, or the University’s Diversity Partner before any disclosures are made.

8.10 Verification of Attendance, Employment and Qualifications

8.10.1 The University will often be contacted by employment agencies, prospective employers and other third parties to verify details about a student or to ask if a member of staff is employed at the University. For the avoidance of doubt, enquiries such as these are distinguished from a request for a reference, for which separate guidance is provided.

8.10.2 As referred to in 8.6.1 ii) above, requests for verification of personal data will be dealt with under FOISA and should be submitted as required in 8.6.4 and 8.6.5 above. On receipt, the following will be considered:
i) whether an exemption should be applied under s.38 of FOISA; and

ii) any notice received from the individual under s.10 of the DPA 1998 asking the University not to process their data, as this would be likely to cause them damage and/or distress

However, in circumstances where the University has already fairly and lawfully publicly disclosed the information requested e.g. by publication of award results by student name in the media or by inclusion of the member of staff's name in an external staff directory and in the absence of a s.10 notice, then the exemption should not be applied.

8.10.3 Obtaining written consent from the individual concerned is the best way to proceed on this, but it is possible to provide confirmation without seeking consent. The DPA 1998 allows disclosure of data to a third party if it is for the purposes of a legitimate interest pursued by the third party and only if disclosure would not prejudice the "rights and freedoms or legitimate interests of the data subject". E.g. confirming a student's attendance to a formal financial sponsor, **provided** that there is evidence of a contractual arrangement, could be considered as a "legitimate interest" pursued by the sponsor and at the same time confirmation would also be in the legitimate interests of the student.

8.10.4 Where there is a legal right for the third party to receive confirmation, a disclosure would be justified. Under these circumstances, a bona fide third party requesting the confirmation should be prepared to explain the legal basis for their enquiry. If in doubt Governance Services should be consulted before any disclosure is made.

8.10.5 If the subject is not known to the University, the DPA 1998 does not apply since no personal data is being held by the University and therefore this can be confirmed to the requester.

8.11 False Qualifications Claims

From time to time University staff may be asked to confirm the award or qualifications of a student, former student or member of staff, which may have been falsely claimed. As referred to in 8.6.1 ii) above, these requests should be handled under FOISA. Relevant staff must check first that any such enquiry is bona fide and in the legitimate interests of the enquirer to make by asking the enquirer to:

- submit the request in a letter on headed notepaper, which has been signed by an authorised representative of the organisation and addressed to a named member of University staff
- provide details of the personal data sought and the purpose and justification for the request, so that the University can consider whether the request is necessary and proportionate

Once these requirements have been met, the request should then be handled as follows:

8.11.1 In cases where the individual has never had a relationship with the University, it is permissible to confirm that the University holds no record of that individual.

8.11.2 If the individual has studied at the University and e.g. they failed a programme of study but are claiming that they were given an award, the enquiry should be directed to the Head of Student Administration, who will confirm only that the student has not achieved the award claimed and no disclosure will be made about any other award.

8.11.3 Where the qualifications of a member of staff are questioned, this should be directed to the relevant Dean of School or Service who should seek advice where necessary from the Director of Human Resources or his/her Depute.

8.11.4 In all cases where it is established that a false claim has been made, the University will consider any appropriate action to be taken with regard to the claimant. This may include: requesting, where address details are held, that the claimant ceases to make incorrect and false claims, notifying other institutions from which the individual claims to have received an award or taking legal action where an individual persists in their false claim.

8.12 Further Information on Data Sharing

The UK Information Commissioner has published a Data Sharing Code of Practice