Edinburgh Napier UNIVERSITY

DATA PROTECTION CODE OF PRACTICE

Revised April 2012

CONTENTS

You can also view the Data Protection Code of Practice online.

1. FOREWORD AND ACKNOWLEDGEMENTS

Edinburgh Napier University's Data Protection Code of Practice was based on a JISC Model Code (2008) and has been revised by members of the University's Information Governance Group and other key staff to include:

- New legislation and developments in case law
- Codes and other guidance issued by the UK Information Commissioner (ICO)
- Updated University guidance documents on the application of the Data Protection Act 1998 (DPA) and other resources

The University's Code concentrates on key issues of concern to the University, reflects our agreed policies and procedures, provides links to these where appropriate and to other resources which have been developed.

Governance Services publishes other related materials on Data Protection, including the University's Data Protection Policy statement.

The ICO is responsible for enforcing and overseeing the DPA and publishes information, tools and resources at: www.ico.gov.uk

In addition to JISC and the contributors to the model Code, Edinburgh Napier University gratefully acknowledged other material originally incorporated from guidance published by the University of Edinburgh, University of Brighton and the University of Essex.

This revised Code was approved by the Risk, Resilience and Audit Monitoring Committee on 27 March 2012.

H Mizen
Governance Officer (Data Protection and Legal)
Governance Services
April 2012

2. KEY DEFINITIONS

Unless otherwise stated these are taken from the DPA 1998

2.1 Data

'Data' falling under the DPA 1998 is defined as information which is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose, or is recorded with the intention that it should be processed by means of such equipment
- recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
- not covered by the first two categories but forms part of an 'accessible record'

2.2 Personal Data

Any information that relates to an identified or identifiable person (the Data Subject), or which in combination with other information in the possession of, or that is likely to come into the possession of, the Data Controller would permit their identification. The DPD 1995 further defines an identifiable person as one who can be identified by reference to 'an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

The ICO provides Guidance on the factors to be considered in determining whether information is personal data.

2.3 Sensitive Personal Data

Personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences.

2.4 Data Subject

A living individual who is the subject of personal data. Dead people cannot be data subjects, nor, in the UK and most other EU Member States, can 'legal individuals', such as companies.

2.5 Data Controller

A person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. The fact that an individual or institution holds or processes personal data does not make them a Data Controller, if they do not determine the purpose and manner of that holding or processing.

- Data Controller in Common: Data Controllers who share personal data on Data Subjects for different purposes are referred to as 'Data Controllers in Common'. Each Data Controller remains individually responsible for the processing they have carried out on the personal data.
- Joint Data Controller: Data Controllers who share personal data on Data Subjects for the same purpose, and who would be jointly liable for any breach under the DPA 1998, are referred to as 'Joint Data Controllers'.

2.6 Data Processor

Any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller. An employee of the Data Controller is regarded by the DPA 1998 as constituting part of the Data Controller. Data Controllers need to ensure that their relationship with a Data Processor is governed by a formal Data Processing Agreement.

2.7 Data Processing

Obtaining, recording or holding the data or carrying out any operation or set of operations on the data. This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. It is irrelevant whether these actions are manual or automated.

2.8 Data Processing Agreement

A contract between a Data Controller and a Data Processor, which will be entered into before the Data Processor begins processing personal data on behalf of the Data Controller, and which set out the responsibilities of both parties in respect of that processing, as well as any indemnities required by the parties.

2.9 Records

Information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business. (Records Management Standard BS ISO 15489)

2.10 Fair Processing Notice

The notice used by a Data Controller to provide a Data Subject with information relevant to the processing of their personal data, usually at the time of its collection. The University has fair processing notices for staff and students.

2.11 Consent

Consent or explicit consent are not defined in the Act. The Data Protection Directive on which the DPA 1998 is based defines the data subject's consent as:
"Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

These factors should be considered:

- If a Data Subject's consent is to be relied on to provide a criterion for lawful processing, then the fact of consent cannot be simply assumed by the University (e.g. where a form is sent stating that in the absence of a negative response from a Data Subject their consent will be assumed).
- For 'explicit consent' to be relied on to provide a criterion for lawful processing, some clear form of affirmative action (e.g. written consent, clicking on an 'I accept' button on a webpage) is likely to be required.
- A Data Subject must also have some genuine control over whether or not the lawful processing takes place
- Consent may be withdrawn by the Data Subject at any point

In Scotland there is an automatic presumption that a person of 12 years or more is of sufficient age and maturity to understand and exercise their rights under the DPA 1998.

The University has a template consent form for subjects' use.

2.12 Legitimate Interests

The DPA 1998 allows, as a criterion for lawful processing of a Data Subject's personal data, the fact that the processing is necessary for the purposes of legitimate interests pursued by the University, or by a third party or parties to whom the data are disclosed. However, this condition cannot be satisfied if the processing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the Data Subject whose data is being processed. This criterion applies only to circumstances where the personal data to be processed does not contain sensitive personal data. Where sensitive personal data is to be processed, the University must satisfy an additional criterion for lawful processing to take place.

3. INTERACTION WITH OTHER LEGISLATION

3.1 Freedom of Information (Scotland) Act 2002 (FOISA 2002)

The Freedom of Information Act gives a general right of public access to all types of 'recorded' information held by public authorities, set out exemptions from that general right, and places a number of obligations on public authorities. FOISA applies only to Scottish public authorities (which includes Universities) and not to private entities. Both the DPA 1998 and FOISA relate to aspects of information policy and overlap where personal information is considered for disclosure. The Scottish Information Commissioner oversees FOI in Scotland but the UK Information Commissioner (ICO) oversees data protection in Scotland.

Public authorities have two main responsibilities under these Acts:

- They must produce a 'publication scheme', in essence, a guide to the information they hold which is publicly available
- They must deal with individual requests for information. Under the DPA 1998 individuals have a subject access right as regards their personal data, held on computer, and in some paper files. FOISA additionally permits individuals to request all other types of information that public authorities hold, subject to specific exemptions in the Acts

FOISA & DPA 1998

FOISA also extends the data subject access rights that already existed under the DPA 1998, to include all "recorded information held by a public authority" not otherwise covered by the DPA 1998 (in other words, any personal data not held on computer or in a relevant structured manual filing system). FOISA states that information is "held" by a public authority if:

- It is held by the authority, otherwise than on behalf of another person, or
- It is held by another person on behalf of the authority

While the FOISA amendments to the DPA 1998, in principle, make all personal data held by the University available to data subjects, regardless of the form in which it is held, there are important limitations upon the rights granted:

- Recorded information held in manual form outside of 'relevant structured manual filing systems' by the University is exempt from all of the data processing principles and obligations, apart from the requirement of accuracy; rectification, blocking, erasure or destruction of inaccurate records; the subject access provisions; and the right to compensation for damage or distress
- There is a partial exemption from the subject access provisions for the new category of data. This exemption is provided by dividing the new category of information into 'structured' and 'unstructured information'; and restricting access to the "unstructured information" to that which is described by the data subject and falls within specific costs limits
- A final exemption for the new category of data absolutely exempts personnel matters (i.e. information about "appointments or removals, pay, discipline, superannuation or other personnel matters"). However, the fact an exemption exists under the DPA 1998 does not mean that the University will have to use it.

Handling requests

A request by an individual for information about him or herself is exempt under FOISA and should be dealt with as a 'subject access request' under the DPA 1998. In certain circumstances, such a request may involve the release of associated third party information. Any information about an individual that is exempt from disclosure to them under the DPA 1998 is also exempt under FOSIA, subject to consideration of the public interest by the University (qualified exemption).

Where an applicant specifically requests information about a third party, or where responding to a request for information would involve the disclosure of personal information about a third party, the request falls within the remit of the FOISA. However, the University must apply the Data Protection Principles when considering the disclosure of information relating to living individuals and must not release third party information if to do so would mean breaching one of the Principles.

Where the disclosure would not breach the Principles, the University may release the information. However, if the third party has served notice under s.10 DPA 1998 that disclosure would cause them unwarranted substantial damage or distress, or the third party would not have a right to know about the information relating to them or a right of access to it under the DPA 1998, the University is required to consider whether release of the information would be in the public interest.

3.2 Human Rights Act 1998 (HRA 1998)

The Human Rights Act 1998 (HRA 1998) incorporates the European Convention on Human Rights into UK law. The Act does three main things:

1. Makes it unlawful for a public authority, such as a government department, local council or the police to breach the European Convention on Human Rights, unless an Act of Parliament meant it could not have acted differently
2. Permits individuals bringing an action for alleged breach of their rights to have the case heard by a UK court or tribunal rather than having to go to the European Court of Human Rights in Strasbourg
3. Requires UK legislation to accord with the rights set out in the Convention

The main provision of the HRA 1998 relevant to data protection is Article 8, which states:

- Everyone has the right to respect for his private and family life, his home and his correspondence
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

The Act is designed to apply human rights guarantees beyond the obvious governmental bodies. S.6 HRA 1998 identifies two distinct categories of "public authorities" which would have a duty to comply with the Convention rights:

- "Pure" public authorities (such as government departments, local authorities, or the police) are required to comply with Convention rights in all their activities, both when discharging intrinsically public functions and also when performing functions which could be done by any private body. s.6(3)(a)
- "Functional" public authorities who exercise some public functions but are not "pure" public authorities are required to comply with Convention human rights when they are exercising a "function of a public nature" but not when doing something where the nature of the act is private. s.6(3)(b)

Only those bodies which fall within either of these categories ("pure" or "functional" public authorities) have a *direct* obligation under the Act to comply with Convention rights. The precise nature of particular HE institutions under these categories appears to remain unclear - unlike FOISA, the HRA 1998 contains no listing of either 'pure' or 'functional' public authorities.

The HRA and the DPA 1998

From a data protection point of view, in circumstances where an HE institution was not directly breaching the HRA 1998, UK courts are required to comply with Convention rights, and obliged to interpret legislation in accordance with Convention rights. Therefore, breaches of the DPA 1998 could give an indirect cause of action to individuals seeking to claim that their Article 8 rights were being breached. The requirement of respect for private and family life, home and correspondence under Article 8 will influence judicial interpretations on DPA 1998 related issues such as the protection of personal information and the right to private communications. Article 8 is not an absolute right but any interference with the right must be in legitimate pursuit of fair and lawful purposes and must be demonstrably necessary and proportionate to achieve those purposes.

It should be noted that the HRA 1998 may require the University to balance an individual's claims for breach of privacy or misuse of private information under Article 8 ECHR against countervailing arguments based on the Article 10 ECHR rights relating to freedom of expression, including the freedom to receive and impart information and ideas.

3.3 Regulation of Investigatory Powers Act 2000 (RIPA 2000)

The Regulation of Investigatory Powers Act 2000 (RIPA 2000) provides, in conjunction with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR 2000), grounds for the lawful interception of communications, including telephone and computer communications (e.g. e-mail, instant messaging). However, personal data collected under the RIPA and the LBPR must be processed in accordance with the requirements of the DPA 1998, unless elements of that processing are specifically exempted e.g. processing of personal data collected under the RIPA/LBPR for the purposes of law enforcement (s.29, DPA 1998) or national security (s.28, DPA 1998) is exempted from parts of the Act.

3.4 Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011(PECR 2011)

The Privacy and Electronic Communications Regulations were originally introduced in 2003 to regulate direct marketing activities by electronic means (by telephone, fax, email or other electronic methods). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and 'spyware'. The Regulations complement the DPA 1998 in the regulation of organisations' use of personal data and in ensuring appropriate safeguards for individuals' rights and privacy. The Regulations apply different rules to individual subscribers and corporate subscribers, although some rules apply to both. Where personal data is used the DPA 1998 always applies and the Regulations cannot be used to avoid the requirements of the DPA 1998.

The European Directive on which the Regulations are based was revised in 2011. As a result the existing Regulations in the UK were amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

Many of the 2003 Regulations have stayed the same, but there are some important changes, which include:

- new rules for websites using cookies and similar technologies (see section 9 of this Code of Practice);
- the introduction of new powers for the UK Information Commissioner (ICO) to serve a monetary penalty on an organisation when very serious breaches of the Regulations occur; and
- the introduction of new powers for the ICO to investigate breaches of the Regulations by obtaining information from certain third party organisations.

The parts staying the same include most of the rules on marketing by live phone call, automated phone call, fax, email and text message.

'Direct marketing' means 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals' (s.11 DPA 1998). The ICO considers "'direct marketing' as covering a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals."

Where the University wishes to communicate via electronic means with individuals, such as prospective students (e.g. marketing the University) or alumni (e.g. fundraising) they must comply with the following rules in order to use these media for marketing communications to individual subscribers:

- **automated calling systems:** the University must have prior consent. Prior consent means that the individual has given some positive indication of intention. This does not necessarily require a tick box "opt-in" e.g. if the individual has clearly indicated their consent to the purposes and to the receipt of marketing communications in some other fashion i.e. clicking on an "Accept" button at the end of a marketing notice

- **faxes**: the University must have prior consent, and check with the Fax Preference Service on a regular basis, unless the individual has notified the University that such communications can be sent ”for the time being”

- **live voice telephone calls**: the University must honour individuals' "Do not Call" requests, and check with the Telephone Preference Service on a regular basis, unless the individual has notified the University that such communications can be sent 'for the time being'

- **e-mail/SMS:** the University must have the opt-in consent of subscribers OR meet the soft-opt-in test:
  - Contact details are obtained during negotiation or sale of goods or services to the recipient AND
  - marketing is conducted by the same entity as previous dealings with the individual AND
  - marketing relates to "similar products and services" AND
  - an opt-out mechanism is provided at the point of data collection and is provided with each new communication.

Enforcement of PECRs

The Privacy and Electronic Communications Regulations are enforced by the ICO. Following the introduction of significant new powers, the Information Commissioner may now impose a civil monetary penalty of up to a maximum of £500K if a business is found to have committed a very serious breach of the Regulations. In other cases an Information Notice requesting further information or an Enforcement Notice will be issued and a fine may be imposed for breach of an Enforcement Notice.

3.5 The Electronic Commerce (EC Directive) Regulations 2002

The e-Commerce Regulations 2002 include a requirement that the recipient of an e-Commerce service, including direct marketing, must be provided, in a form and manner that is easily, directly and permanently accessible, with certain information including:

- The name of the service provider i.e. the University
- The geographic address at which the service provider is established
- The details of the service provider, including staff email address, which make it possible to contact him rapidly and communicate with him in a direct and effective manner

The purpose of this requirement is to ensure that individuals are able to effectively utilise their consumer protection and other rights, including those granted under the DPA 1998 and PECR 2003 as amended in 2011, by providing them with the necessary information about whom to enforce those rights. The Regulations do not prescribe how the requirement to make information "easily, directly and permanently accessible" should be met.

3.6 Equality Act 2010

The Equality Act became law in October 2010 and has two main purposes: to harmonise discrimination law and strengthen the law to support progress on equality. It replaced previous legislation (such as the Race Relations Act 1976 and the Disability Discrimination Act 1995) and ensures consistency in what employers need to do to make the workplace a fair environment and to comply with the law. The Act places a new duty on certain public bodies to consider socio-economic disadvantage when making strategic decisions about how to exercise their functions. It also extends the circumstances in which a person is protected against discrimination, harassment or victimisation because of a protected characteristic. There are nine protected characteristics:

- Age
- Disability
- Gender reassignment
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

The Act places duties on public authorities to collect key sensitive personal data such as ethnicity, disability and gender. The University may also be required to collect protected characteristic data by HESA at some point in the future. It should be noted that this may be withheld where it has the potential to identify individuals or a group with a particular protected characteristic.

3.7 Other Legislation

The DPA 1998 itself does not oblige institutions to disclose personal data to specific third parties, but states that personal data is exempt from the Act's non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law, or by the order of a court.

Certain third parties can thus require disclosure of an individual's personal data by the University in order to meet other legislative requirements. Further guidance on this is in Section 8: Data Sharing.

4. PROCESSING OF PERSONAL DATA BY EMPLOYEES

4.1 Processing under the University's Notification to the UK Information Commissioner

4.1.1 The University is a data controller for the purposes of the Act and as such is required to notify the Office of the UK Information Commissioner (ICO) of the purposes for which personal data is processed.

4.1.2 This notification should cover University employees who are processing personal data on behalf of the University and as a legitimate part of their employment e.g. in research, teaching, consultancy or administration.

4.1.3 This applies whether they are processing the data at work or home and either on an occasional or regular basis. All work related documents are University records **irrespective** of where they are physically stored.

The purposes for which the University processes data may be viewed for at: http://www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=5619734

4.2 Employee Access to and Use of Personal Data

4.2.1 All personal data collected, held and processed in any medium including on computer, online and in structured and unstructured manual files, is subject to the DPA 1998 and the University's Code of Practice.

4.2.2 All employees' access to and use of personal data is limited strictly to the purposes legitimately associated with their roles.

4.2.3 All employees must ensure that personal data is not communicated to other persons or bodies unless:

- required to do so by law
- for the proper purposes of University business; or
- with the consent of the individual concerned.

Any such disclosures of information must be consistent with the Act, the University's notification under the DPA 1998, this Code of Practice and any associated guidance.

4.3 Temporary Staff

Where a temporary member of staff is engaged, it is the responsibility of the member of staff who has arranged the temporary employment to ensure that:

- any such temporary staff member signs an Oath of Confidentiality, on the day they commence employment at the University before being given access to any personal data.
- the provisions of section 4.5 below are strictly adhered to

4.4 Sensitive Personal Data

4.4.1 Some personal data is classed as sensitive personal data. This data is subject to further and more stringent regulations under the DPA 1998, which require that it may be processed only in certain circumstances.

4.4.2 Personal data is regarded as sensitive if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health;
- sexual life;
- commission of offences or alleged offences.

4.4.3 Sensitive personal data may only be processed if at least one of the following conditions is met:

- Explicit consent has been given by the individual
- Processing is required to comply with employment legislation
- Processing is necessary to safeguard the vital interests of the individual or another person
- The information has already been made public by the individual
- Processing is necessary in connection with legal proceedings
- Processing is necessary for the administration of justice
- Processing is necessary for medical reasons
- Processing is necessary for ethnic monitoring.

Further guidance on processing sensitive personal data is provided in Section 8 of this code.

4.5 Responsibilities

4.5.1 All Heads of Schools, Service Areas and other University staff who are responsible for employees processing personal data must ensure that:

- there is a level of security in place which is appropriate to the risks represented by the processing and the nature of the data to be protected
- security of data is assured irrespective of where or by whom data is stored or processed throughout the whole procedure, including the transmission of that data
- an employee who is required to have access to the Student Records System, SITS in order to carry out their duties and who is also an enrolled student at the University, has signed the relevant oath of confidentiality
- data has been retained in accordance with the University's retention schedules and may be retrieved in response to a data subject access request

4.5.2 All employees processing personal data are responsible for ensuring that:

- appropriate measures are taken to prevent personal information (in whatever format) from being divulged to unauthorised persons
- appropriate care is taken in disposing of printed information containing personal information in accordance with the University's guidance on the Safe Disposal of Confidential Waste
- within individual work areas, the current general guidance on handling personal information is followed, together with any specific additional measures that may apply
- the Governance Officer (Data Protection and Legal) is informed of any personal data that is being or is intended to be handled, which is not notified, or of any changes in the way the data is being handled, which might affect the University's notification under the Data Protection Act. For anyone handling personal data that they do not themselves control, this responsibility will be met by checking with the person who controls the data.

4.5.3 Employees are not permitted to remove personal data from the University with the intention of processing this data elsewhere except where:

- the personal data is used or processed to carry out the duties of the member of staff and for no other purpose and such use is recognised and authorised by the relevant Head of School or line manager

- the processing is carried out only for a purpose included in the University's notification with the ICO
- the University's Information Security policy and Manual Data Security policy are strictly complied with to ensure that adequate security is maintained.

4.5.4 Any failure to observe the responsibilities referred to in 4.2 to 4.5 above will be regarded seriously and may result in disciplinary action being taken.

4.6 Processing Outside the University's Notification

4.6.1 Where employees process personal data for which the University is not the data controller e.g. for their own personal or domestic purposes this will be exempt from notification.

4.6.2 For other purposes e.g. commercial exploitation of personal data unrelated to the University's notification for University academic work, this may require separate notification to the ICO by the individual. Guidance on this must be sought from the relevant Head of School or the University's Governance Officer (Data Protection and Legal).

5. PROCESSING OF PERSONAL DATA BY STUDENTS

5.1 The University's Responsibility

The University is responsible for personal data when it is the data controller for that data i.e. where the University determines the purposes for and the manner in which any personal data is to be processed. For information on the processing of data by students where this is not for University purposes please consult the Governance Officer (Data Protection & Legal).

5.2 Permitted Use

A student is only permitted to use personal data for a University related purpose with the knowledge and express consent of an appropriate member of staff. For research purposes this would normally be a postgraduate supervisor or the person responsible for teaching the relevant undergraduate class or course. For administrative purposes this will be on the express authorisation of the line manager or supervisor of the project on which the student is employed.

5.3 Staff Responsibilities

Where students process data for the University's purposes, the relevant staff must ensure that:

- The processing is covered by the University's notification with the UK Information Commissioner (ICO)
- The Governance Officer (Data Protection and Legal) is informed of any personal data that is being or is intended to be handled, which is not notified, or of any changes in the way the data is being handled which might affect the University's notification under the Data Protection Act.
- Students are complying with the Data Protection Principles, this Code of Practice, including where relevant Section 6: Use of Personal Data in Research, the University's Information Security and Manual Data policies. The use of personal

data by students should be limited to the minimum consistent with the achievement of academic or corporate objectives. Wherever possible data should be anonymised so that students are not able to identify the subject.

- Written authority from the relevant Head of School or Service has been sought before a current, employed student is given access to the Student Record System, SITS and the relevant oath of confidentiality has been signed
- Data has been retained in accordance with the University's retention schedules and is capable of being retrieved in response to a data subject access request
- Students are made aware that data subjects have a right of access to their personal data and to object to the accessing, processing and disclosure of their personal data whether held on computer or in manual files where the data subjects feel it may cause them significant damage or distress.

5.4 Student Access to and Use of Personal Data

5.4.1 Students who are authorised to hold or process personal data on computer, online or in manual format are required to:

- Sign an oath of confidentiality at the start of their employment or research project
- Comply with this Code of Practice, the Data Protection Principles, the University's notification with the ICO and relevant University policies.

5.4.2 All students processing personal data are responsible for ensuring that:

- appropriate measures are taken to prevent personal information (in whatever format) from being divulged to unauthorised persons
- appropriate care is taken in disposing of printed information containing personal information in accordance with the University's guidance on the Safe Disposal of Confidential Waste
- within individual work areas, the current general guidance on handling personal information is followed, together with any specific additional measures that may apply

5.4.3 Research students are not permitted to remove personal data in any format from the University without the express written authorisation of their academic supervisor.

5.4.4 Employed students are not permitted under any circumstances to remove personal data in any format from the University.

5.4.5 Any failure to observe these responsibilities, including the inappropriate or unauthorised disclosure of personal data, may lead to disciplinary action being taken under the Student Conduct Regulations.

6. USE OF PERSONAL DATA IN RESEARCH

Introduction

The Act sets out to ensure that researchers may only process data about other living individuals where they have a clear legal purpose for doing so and subject to certain prescribed exemptions, the use of personal information for research falls within its remit. Staff and students engaged in research at the University are obliged therefore to comply with the requirements of the eight data protection principles , this Code of

Practice and any associated guidance, when collecting and processing personal data for research purposes. In addition to computerised records these requirements apply to written records held in a structured filing system, digital and microfiche records and video recordings. Students who are authorised to hold or process personal data on computer, online or in manual format are also required to sign an Oath of Confidentiality at the start of their research project

6.1 Factors to Consider in Using Personal Data for Research

There are two options to consider in using personal data for research:

a) Comply with the Act; or
b) Anonymise the data to be used so that it no longer falls within the Act's definition of personal data.

6.1.1 Option a) means that all the requirements of the Act must be met and sections 6.2 to 6.5 below apply.

6.1.2 Option b) means that the personal data to be used must be completely anonymised. This will only be achieved if it is impossible to identify the subjects from that information together with any other information that the University holds or is likely to hold. If that is the case then the data may be used without making arrangements to comply with the Act since the data will no longer fall within the Act's definition of personal data.

6.2 Exemptions for Research Purposes

6.2.1 Where processing for research purposes (including statistical or historical purposes) is not used to support measures or decisions targeted at particular individuals, and will not cause substantial distress or damage to a data subject, the data gathered for research purposes is exempt from being processed in accordance with the second and fifth data protection principles.

6.2.2 This means that personal information can be:

- processed for purposes other than those for which it was originally obtained. e.g. researchers can keep records of questionnaires and contacts so that the research can be re-visited at a later date or so that the information can be re-analysed in support of a research project looking at an associated area; and
- held indefinitely

6.2.3 Whilst an exemption may be applied researchers must be aware that there is no blanket exemption from observing the remaining Data Protection Principles. This means therefore that:

- Research subjects should be informed of any new data processing purposes, that the University is the Data Controller and any disclosures that may be made
- Research subjects must be able to meaningfully exercise their right to object to the data processing on the ground that it would cause or has caused them significant damage or distress
- Requirements for appropriate security of data must be observed, particularly those for the security of sensitive data
- Data may not be transferred to researchers outwith the European Economic Area (EEA) unless:
  - that country has adequate data privacy protections

- the explicit consent of the subject(s) has been obtained; or
- there is an appropriate data protection contract with the data recipient

6.2.4 There is also an exemption from an individual's right of access where:

- Personal data is not processed to support measures or decisions with respect to particular individuals
- Personal data is not processed in a way that substantial damage or distress is or is likely to be caused to any individual
- The research results, or any associated statistics, are effectively anonymised

6.2.5 However, the University may still choose to disclose the information to the data subject, unless by doing so this would breach another individual's data protection rights.

6.2.6 The legislation recognises that the value of access to personal data in research may outweigh an individual's desire to exercise a high level of control over the use of their data. Researchers wishing to use sensitive personal data should be able to do so, if they can demonstrate a significant public interest, they have secured the approval of the University Academic Ethics and Research Governance Committee and they adhere to the procedural safeguards required by law.

6.3 Factors to be Considered When Processing Personal Data for Research Purposes

6.3.1 Researchers are required to carry out an adequate review in advance of processing, to ensure that the requirements of the Act and in particular the eight Data Protection Principles can be adhered to.

6.3.2 Research subjects are to be fully and clearly informed about the purpose of the research for which their personal data will be collected, how their data will be used and who will have access to it.

6.3.3 Adequate security measures, consistent with the sensitivity of the personal data and the format in which it is held, must be in place to ensure that personal data is protected from unauthorised access, accidental loss, damage or destruction. These measures should be communicated to the subjects as part of the information given to them relating to the nature of the research project and how data about them will be used.

6.3.4 Research subjects have a right to object to the processing of their personal data where they can establish that such processing would cause them significant damage or distress.

6.3.5 Researchers must be aware that processing of personal data which has been coded or anonymised, but for which links to an individual can still be made by reference to a key to the code or to other identifiers, remains subject to the DPA 1998, this Code of Practice and any associated guidance.

6.3.6 Subject to specific procedures, the DPA 1998 provides all individuals with the right to request access to intelligible copies of personal data about them where they are identified as the data subject. Personal information gathered as part of research activity is exempt from such a disclosure where the data is managed

in accordance with the relevant data protection principles and the results of the research are not made available in a form that identifies the data subject(s).

6.3.7 Particular care must be taken when the processing involves sensitive personal data, for which the DPA 1998 imposes more stringent conditions. See Section 4.4 for further guidance.

6.3.8 Research carried out for the NHS or under contract for a commercial organisation is subject to notification by that body and to that organisation's own Data Protection policies. However, any data which has not been fully anonymised and is downloaded with permission from an NHS or other external system to a University system constitutes a University database and has to be registered and treated as such.

6.3.9 A review of the processing must be carried out at least annually to ensure that compliance with the DPA 1998 is being maintained and documented.

It is recommended that researchers refer to the Researchers' checklist before embarking on any research project.

6.4 Processing Sensitive Personal Data

6.4.1 The processing of sensitive personal data may be carried out provided the conditions prescribed in the DPA 1998 are met e.g. explicit consent has been obtained. Further guidance is available in Section 4.4 of this Code.

6.4.2 In addition, the Data Protection (Processing of Sensitive Personal Data) Order 2000 expressly permits processing for research purposes 'in the substantial public interest' where the data is not used to support measures or decisions targeted at particular individuals without their explicit consent; and no substantial damage or distress is caused, or is likely to be caused, to any person by the keeping of that data.

6.5 Online Research with Human Subjects

6.5.1 For many on-line research projects, existing ethical guidelines will already meet the requirements of the data protection legislation. However researchers seeking to gather research data online must be aware that this environment generates significant amounts of background information e.g. data logs, IP address collection, cookies and caches.

6.5.2 Where internet research tools and computer systems are used, researchers are required to identify and address potential technical and administrative problems e.g. poor research tool configuration and inappropriate levels of system security or integrity.

6.5.3 Researchers are thereafter required to seek confirmation from the University's Research Office, Programme Leader or Project Supervisor that any proposed on-line project involving personal data meets the University's ethical and data protection guidelines.

6.6 Provision of Research Data to Third parties

The University is required to consider requests for research data which are not subject to the research exemption under the Freedom of Information (Scotland) Act 2002. The following factors must be considered in order to comply with the DPA 1998:

- Can individuals be identified from personal data in the data requested or are they likely to be identifiable from that data in combination with other information likely to be available to the third party.
- If there is a risk of identification of an individual, can that risk be removed by:
  - Redaction of the data
  - Provision of the data in statistical form
  - Provision of the data in statistical form after it has been appropriately anonymised to disguise subjects' identities when information consists of low numbers
- Is the cost of providing the data in appropriately anonymised form reasonable.

Advice and guidance must be sought from the University's Governance Officer (Records Manager) before any data is disclosed.

7. SECURITY OF PERSONAL DATA

Introduction

The University is required under the DPA 1998 to have in place an institutional framework designed to ensure the security of all personal data, in whatever format, from collection through to destruction. All staff, students and authorised visitors who deal in any way with personal data have a responsibility under the DPA 1998 to take all appropriate security measures to protect data against unauthorised loss, destruction, corruption or disclosure. The level of security used should be appropriate to the degree of harm that could occur if the personal data is misused.

Personal data should only be processed in accordance with:

- the eight data protection principles
- the University's notification with the UK Information Commissioner
- This Code of Practice, relevant University policies and associated guidance

Any failure to comply with the above requirements may result in disciplinary action being taken.

7.1 Electronic Data

Information Systems play a major role in supporting the day to day activities of the University. Staff and students using the University's systems must comply with the following University Information Security Policies:

- Overall Policy
- User Policy
- Monitoring and Logging Policy

Information Services publish further information and tips on security of electronic data in their Introduction to Information Security.

7.2 Manual Data

All personal data must be stored in a secure environment with controlled access. The level of security to be applied should be agreed after a basic risk assessment has been carried out.

Appropriate secure environments include:

- locked metal cabinets with access to keys limited to authorised personnel only
- locked drawer in a desk (or other storage area) with access to keys limited to authorised personnel only
- locked room accessed by key or coded door lock where access to keys and/or codes is limited to authorised personnel only

Further guidance on risk assessments and appropriate security measures is available in the University's Manual Data Security Policy

7.3 Contractors, Vendors and Suppliers

Vendors, contractors or suppliers will at times be required to have access to areas in which personal data may be stored or processed. In certain circumstances it may also be necessary to allow contractors access to personal data (e.g. computer engineers) in the course of maintenance or repair work.

7.3.1 Contractors

Staff responsible for securing the services of contractors are required to ensure that the contractors are:

- Controlled, documented and required to wear some form of identification
- Restricted from unnecessary access or admittance to areas where personal data is held or processed
- Required to sign an oath of confidentiality where access to personal data is unavoidable

7.3.2 Vendors and suppliers

Staff responsible for vendors and suppliers visiting their areas are required to ensure that vendors and suppliers are:

- Controlled, documented and required to wear some form of identification
- Escorted throughout the area by the staff member they are visiting
- Restricted from unnecessary admittance to areas where personal data is held or processed

Staff and students are asked to challenge or report to security, individuals they may see without the proper credentials, in areas where personal data is held or processed.

7.4 Students

7.4.1 The University's guidance on the student processing of personal data is available in Section 5 of this Code. The University does not envisage that many students will have access to or be processing personal data for which the University is the Data Controller; this is particularly so for undergraduate students.

7.4.2 Employed students are not permitted under any circumstances to remove personal data in any format from the University. However, research students in certain subjects, such as Nursing and Midwifery and certain life and social sciences, may be permitted to access or process personal data for which the University or a University's partner is the Data Controller, in the course of their studies or research.

7.4.3 University staff who have authorised this processing of data are responsible for ensuring that such students are given formal training in their and the University's obligations under the DPA 1998 and advised on appropriate security measures. This could be carried out as part of the University's ethical review process for postgraduate research projects.

7.4.5 In particular students must be made aware of the following:

- In the case of data for which the University is the data controller, the purposes for which the data has been collected, including the parties to whom disclosure may legitimately be made, and that disclosure may not be made to other parties, unless one of the exemptions in the DPA 1998 applies
- In dealing with personal data, for which the University is the Data Controller, requests for disclosure under one of the exemptions in the DPA 1998 (e.g. law enforcement) are to be referred to the University's Governance Officer (Data Protection and Legal) or Governance Officer (Records Manager).
- In dealing with personal data for which the institution is Data Controller, their access to and use of personal data is for specified authorised purposes only and that any breach of these requirements will constitute an offence under the Student Conduct Regulations
- The requirement to apply and abide by any relevant security requirements contained in agreements with outside bodies who may furnish personal data for university research purposes
- Casual access to personal data, for which the University is the Data Controller, by unauthorised persons by act or omission, is not permitted and that any such acts or omission that do or could lead to unauthorised access or disclosure to unauthorised persons will constitute an offence under the Student Conduct Regulations.
- Failure to adhere to the correct use of applicable access control mechanisms will constitute an offence under the Student Conduct Regulations

7.5 Transfer of Personal Data

7.5.1 All transfers of personal data are to be authorised and/or conducted at an administrative or managerial level appropriate to the type of personal data being transferred and carried out in accordance with any applicable data transfer agreement. Data is only to be transferred in secure conditions which are commensurate with the anticipated risks and appropriate to the type of personal data involved.

7.5.2 Key points to note are:

- It must <u>not</u> be assumed that documents transferred by electronic means e.g. email, web transfers, File Transfer Protocol are secure

- Material containing sensitive personal data, or data that if it should be lost is likely to cause damage or distress to the subjects should always be encrypted to an appropriate standard before it is transferred
- Staff must consider whether data can be anonymised before it is taken off University premises and/or sent either by post or courier
- If this is not possible and it is deemed absolutely necessary to download personal data to physical devices e.g. USB memory sticks, CDs or DVDs then the data must be encrypted.
- Hardcopy data should also be transferred in a manner proportionate to its sensitivity

Information Services publish guidance on data encryption and the software to be used.

A staff checklist on Security of Personal Information is available for summary reference purposes.

7.6 Migration or Update Plans

Staff with responsibility for the future migration or upgrade plans for the University's systems are expected to:

- document in the relevant project plan and subsequently address, the potential effect of hardware, software and operating system upgrades, or obsolescence on personal data processing operations
- consider whether a Privacy Impact Assessment is required.
- carry out successful data transfer tests of existing systems to new systems or file formats before those systems go live and old systems, including manual systems, are discarded

7.7 Back-Up of Personal Data

Key personal data on staff and students is maintained electronically and is therefore backed up in accordance with the University's Information Security Policy. The University is developing guidance on its vital records and the appropriate business continuity measures to be adopted for all electronic and manual data. Although there is currently no policy for maintaining backup copies of manual data, the control measures for access will ensure that manual personal data is kept in an appropriately secure environment where risk of loss or damage is minimised.

Further information is provided in the Manual Data Security Policy

7.8 Working Off-Site, on Home Computers or at Remote Locations

All University staff working from home, either on an occasional or a regular basis must be aware of their obligations under the DPA 1998 and the University's Information Security Policies, when they undertake administrative, research or teaching-related work at home and use information in all formats, including paper files, electronic data, word processed documents and e-mails.

Addressing these issues will also help in compliance with requests received under the DPA 1998 and the Freedom of Information (Scotland) Act 2002. These Acts apply to all paper and electronic information that staff may receive and create as part of their employment with the University, regardless of where that work takes place or where the information is stored.

Staff working from home must not dispose of any paper records containing personal or sensitive data in domestic waste. All such paper records must be returned to the University and disposed of in accordance with the Safe Disposal of Confidential Waste

Further guidance is available from Human Resources in the Home Working Policy, available on the HR Documents intranet page and from Information Services on Remote Access to the Network.

7.9 Destruction of Personal Data

Personal data in both manual and electronic formats should only be destroyed in accordance with the University's agreed retention schedules and Section 20 of this Code. Further advice and guidance may be sought from the University's Governance Officer (Records Manager). Once it has been established that the data may be disposed of, care must be taken to ensure that appropriate security measures are in place to carry this out, whatever the format in which the data is held. Guidance is available on the Safe Disposal of Confidential Waste and the use of Shredding Consoles**.**

7.10 Breach of Data Security

In the event of a breach of data security occurring in the case of either electronic or manual personal data the Procedure for a Breach of Data Security must be consulted.

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 disability discrimination acts, 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 the Governance Officer (Data Protection and Legal), 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 systematic, routine data sharing where the same data sets are shared with the same third party agency or organisation for an established purpose or 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.

8.5.5 If ii) above applies the University must ensure, in a written agreement that:

- the processor only acts on instructions from the data controller; and
- it 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, 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 should be sought from the Governance Officer (Data Protection & Legal) before any data sharing takes place.

8.6 Disclosures without Consent

8.6.1 University staff and students must be aware that third party requests for personal data held by the University should be treated as freedom of information requests and that refusal to supply personal data will have to be justified by reference to s.38 of the Freedom of Information (Scotland) Act 2002. Advice on this may be obtained from the University's Governance Officer (Records Manager) or Governance Officer (Data Protection and Legal).

8.6.2 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 The University will normally require that external agencies seeking the disclosure of personal data in the circumstances referred to at 8.6.2 iii. – vii. above submit their request on headed notepaper and 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
- the relevant DPA exemption or other legislation which authorises the University to release the information
- 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.

8.6.4 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.

8.6.5 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

8.6.6 Disclosures without consent may be made normally only by the University's Governance Officer (Data Protection and Legal), Governance Officer (Records Manager) or other authorised staff in Governance Services, where a central log of disclosures will be securely maintained for reference and inspection purposes.

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 Head 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 the University's Governance Officer (Data Protection and Legal).
- To ask the enquirer to follow up their request with a formal written and signed request, so that this may also be passed to the Governance Officer (Data Protection and Legal) 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 personnel 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 the Governance Officer (Data Protection and Legal) or authorised other 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. Such requests for information should be treated as a FOISA request (as referred to at 8.2.1 above) and the University will need to consider:

i) whether the request should be refused under s.38 of FOISA; and
ii) any notice received from the individual under s.10 of the Act 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.

8.10.2 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.

8.10.3 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 the University's Governance Officer (Data Protection and Legal) should be consulted before any disclosure is made.

8.10.4 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. Staff receiving such a request should check firstly that it is a bona fide enquiry, which it is in the legitimate interests of the enquirer to make by:

- requiring that the enquiry is submitted on headed notepaper and signed by an authorised representative of the organisation making the enquiry
- ensuring that the details of the nature of the personal data sought , the purpose for which it is being requested and the scope of the request are necessary and proportionate

On satisfactory receipt of the above the request should then be handled as follows:

8.11.1 In cases where the individual has never had a relationship with the University as stated at 8.6.3 above, 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 Head 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 a false claim has been made, the University will consider any appropriate action to be taken. 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

9. THE INTERNET, ONLINE SERVICES & WEB 2.0 SERVICES

9.1 University Web Pages

The University has an internet website which is accessible worldwide and a web based intranet which is accessible only to members of the University. Within the set of web pages that make up both types of websites, there are web pages which contain personal data e.g. staff names, images and contact details.

The University has to consider the justification for the display of data and ensure that its use is both necessary and proportionate.

Key Elements:

- The University may use personal data on its web pages without consent where its display facilitates the University's normal organisational functioning and management. This may include publicly available hard copy publications
- Staff are informed in the Staff Processing Statement that certain personal data will be displayed and of their right to object to the use of their data where it would cause them significant damage or distress. Staff should speak to their line manager in the first instance who will consult as necessary in determining whether the damage or distress alleged is a suitable ground for removal
- Sensitive personal data of either staff or students must not be used on University web pages without explicit written consent

9.2 Web Pages Used to Collect Personal Data

9.2.1 Where personal data is collected from web pages e.g. names and addresses of individuals who have requested a University prospectus, it is important that the rationale for the data collection is clear at the point it is requested and that no personal data other than that required for the particular transaction is collected.

9.2.2 Previously, cookies were used on University sites to help users remember their preferences. However in compliance with the Privacy and Electronic Communications (Amendment) Regulations 2011, which will be enforced from May 2012, this approach is no longer used and cookies have either been removed or a logged in service with appropriate explanatory wording will be adopted and consent to the use of cookies sought where required.

9.2.3 University staff who are involved in developing web pages for a purpose that requires collection of personal data must ensure that the following information is provided to the data subject:

- The purpose for which the data is collected
- The recipients (or classes of recipients) to whom the data may be disclosed
- An indication of the period for which the data will be kept (e.g. "while we process your application" or "for the duration of your studies", rather than a specific time period.)
- And any other information that may be required to ensure that the processing is "fair"

In addition, staff must ensure that:

- The data subjects are given the ability to opt out of any parts of the collection or use of data that is not directly relevant to the intended transaction e.g. where an

individual gives their name and address in order to be sent a prospectus and there is follow up research to establish why individuals did not come to the University, the individual should be told about this and be able to opt out of it.
- Subsequent use of the data conforms to the information provided to the data subject and that before any subsequent use that was not disclosed at the time of collection, further consent must be obtained from the individual.

9.3 Internet and Intranet Monitoring

The University requires the ability to inspect all data held on its computer equipment and to inspect all email and other electronic data entering, leaving or within the University network to ensure conformity with:
- The University's Information Security Policies
- Contractual agreements with third parties
- UK legislation

Further guidance is in the University's Monitoring and Logging Policy.

9.4 Web 2.0 Services

Since the use of Web 2.0 services, i.e. Facebook, YouTube, Twitter, LinkedIn and other externally hosted services, almost always involve the use of personal data, there are potential data protection and legal implications for the University, its staff and students

University staff entering into an arrangement with an external service provider for the provision of Web 2.0 services must consider the following data protection risks:

9.4.1 The role of the service provider

The nature of the agreement with the service provider will determine whether the University will be legally responsible for any breaches of the Act. If any of the following apply, the service provider may be deemed to be acting as a data processor for the University and therefore the risk of responsibility for any breaches remains with the University:
- The University has negotiated a specific agreement with the service provider
- The service is branded as a University service
- It is not immediately apparent to users of the service that they are providing data to an external service provider rather than to the University
- Students must sign up to the service as a compulsory requirement of a course or programme
- The service provider can only use the data in ways or for purposes specified by the University

If any of the above situations apply, staff must ensure that there is a data processing agreement in place between the service provider and the University in advance of the service being implemented. Templates to assist with data sharing agreements are available from the Governance Officer (Data Protection & Legal).

The University may avoid becoming legally responsible for the service providers' compliance with the Act by ensuring that it is clearly stated that service providers are separate legal entities. The University would not be determining the purposes for, and

the manner in, which any personal data is to be processed and is not therefore a data controller. This can be achieved by:

- Clearly identifying that the service is provided by an external service provider, both on the site itself, in any supporting institutional documentation (e.g. course handbooks) and in the way that the user access the service (e.g. if students enter the site from WebCT or Moodle, they are given a message that they are now leaving the institution's service and connecting to an external service provider)
- Providing users of the service, such as students, with clear guidance on what information is accessible to and used by the institution, and what information is accessible to and used by the service provider
- Ensuring users of the service sign up to use the service directly with the service provider and not through the University. In this way, each individual can decide on the extent to which they wish to establish their own relationship with the service provider, and can withhold or disclose whatever personal information they wish
- Making participation in and contribution to the service optional for users - e.g. users can choose whether or not to contribute to a research wiki

Staff proposing to use an external service provider should ensure the following:

- Where users are to register individually, that the terms of the service which users will be signing up to are appropriate for the UK legal environment. This is particularly important where use of the service is compulsory for a course.
- Users must not be required to sign up for Web 2.0 services which purport to require them to waive legal protections guaranteed by UK data protection law
- Depending on the nature and extent of use of a service, clear guidance is to be provided either by a short briefing to students or in the relevant course handbook about the data protection implications of their registration. This should include advice on the effective use of privacy enhancing elements of the service, how to unsubscribe and remove personal data from the service

9.4.2 Publication of personal information

Use of some Web 2.0 services may involve requiring users to publish their personal data on the Internet. University staff must be aware that compulsory use of such services by the University, or use of such services in circumstances which place users who do not wish to make such disclosures at a significant disadvantage, may breach the DPA 1998.

This can be avoided by using services which let users conceal their identity, e.g. by allowing the use of aliases. However, withholding of names does not equate to anonymising data and staff should be alert therefore to the risks inherent in requiring the disclosure of so much information that a user can be identified even in the absence of use of their name. Users should be clearly advised on what information will be published and what information will be available on a more restricted basis.

9.4.3 Transferring personal information outside the EEA

Many Web 2.0 service providers are based outside the European Economic Area (EEA), e.g. in the United States. As a result, personal data supplied to those service providers is likely to be processed outside the EEA. While it is acceptable for individuals in the EEA to choose to supply their personal data to non-EEA service providers, the DPA 1998 prohibits the transfer of personal data by data controllers i.e. the University to third parties outside the EEA, unless certain conditions are met.

In circumstances where University staff propose to use Web 2.0 service providers, they must ensure that they know where information that is supplied to the service providers will be processed, so that appropriate measures can be adopted. The following are methods of dealing with personal data transfers outside the EEA in circumstances where a web service is to be used:

- Where users have a choice whether or not to sign up, the University should ensure that its users are adequately informed about the data protection consequences of doing so
- Where the user registers directly with the service, is aware of the overseas transfer, and has control over what information is provided to the service provider, the University must ensure that its users are adequately informed about the data protection consequences of doing so
- When the University is providing user personal data to the service provider as a third party, University staff should consider whether:
    - the country in which the service provider is based has adequate protections for personal data in relation to the proposed transfer (see below)
    - the type of transfer is exempted from the general prohibition on transfers to non-EEA countries
    - there is a need to negotiate a customised agreement with the service provider

When the University is using the service provider as a data processor, the University should negotiate a customised agreement with that service provider. Advice should be sought on this from the Governance Officer (Data Protection and Legal).

9.4.4 Information provision

In order to comply with the DPA 1998 and related legislation, where the University uses an external Web 2.0 service provider to collect information about or contributions from people on its behalf, the relevant staff must provide clear information preferably in the course handbook about:

- How the University or other parties will use the information
- Who will have access to or will retain copies of the information
- What information will be generally accessible over the Internet
- Any cookies that may be downloaded to the user's computer
- Any monitoring of an individual's usage and activity in the service
- The country that hosts the service if it is hosted outside the UK

In addition staff should ensure that:

- Users must give their consent to the use of cookies where relevant and be able to opt out of monitoring.
- If an externally-provided service is designed to appear to be part of the University (e.g. a template has been used to apply the University’s branding to a blog) people who register at that site (e.g. in order to post comments to the blog) understand that they are not just entering into a relationship with the University but also with the service provider.
- Users are given clear information as to what information is available to, and used by, which party.
- They avoid using services where it is not possible to opt out of advertising and marketing emails. In cases where use of the service is compulsory or where the service provider is a data processor acting on behalf of the University, this may

breach the Privacy and Electronic Communications (EC Directive) Regulations 2003. To minimise these risks, users should be given clear instructions on how they can opt out of advertising and marketing activities if they wish to do so.

9.4.5 Information retention

Personal data placed on Web 2.0 services based in non-EEA countries may, in some circumstances, be legally held indefinitely and the service providers may have no legal obligation to remove it. The DPA 1998 requires that the data controllers and data processors should keep information about individuals for no longer than necessary. Staff should therefore:

- Consider carefully if the Web 2.0 services they wish to use will expose the University to liability for breach of the DPA 1998 or expose their users to unwanted long-term personal data disclosure
- Ensure that the Web 2.0 services they wish to use have adequate data privacy guarantees concerning the appropriate removal and disposal of users' personal data after the purpose for which it was collected and processed has ended.

9.4.6 Take Down/deletion

Additionally, where the University has entered into arrangements with Web 2.0 service providers to provide particular services involving the processing of user personal data, the responsible staff should consider whether it is likely to be necessary to take down or delete information that has been posted to the service to prevent the processing of information likely to cause someone substantial damage or distress. Before signing up to a service, staff should consider whether the terms of use and facilities of the external service will enable them to do this quickly, if necessary.

Guidelines for staff and students have been prepared on the legal implications of the use of Web 2.0 services. JISC has prepared a Tutor's Checklist for Staff

9.5 e-Learning systems, Moodle, Virtual Learning Environments and ePortfolios

All e-learning systems will collect and process personal information about students at some point in the process. When a student starts using a virtual learning environment (VLE), they will be generating personal data, examples of which include their personal details, their submitted work and academic results.

In most cases, in respect of a VLE, the data controller for the personal data will be the University. Where the technical provision and administration of the VLE is outsourced to a third party provider, it is still likely that the University will be the data controller, with the third party provider being considered a data processor acting on the University's behalf. In those circumstances the DPA 1998 requires that a contract must be executed in writing between the University and its data processors. In addition to ensuring the security of its own processing, the University must also take steps to ensure that any data processors processing the data on its behalf, are placed under a security obligation.

The data protection issues that are likely to arise from an institutional e-learning system will vary depending on a range of variables and include:

- the developmental process that produced the system
- the nature of the data it is envisaged will be stored in that system
- the range of people who it is envisaged will have access to the data

- in the case of ePortfolios in particular, the means by which learners, rather than the University may make the data available to others.

Further information will be made available on the Moodle Student Help pages when this system goes live.

9.5.1 Data security

It is vital that data in e-learning systems is maintained securely. These systems, their hardware, software, databases and the communications systems on which they are based must be technically robust and secure. Measures which the University must also address include:

- who has access to the system
- what controls are in place over how these people can access the system; and
- how the entire system is governed.

9.5.2 Ongoing compliance

Once an e-learning system becomes operational, the University staff responsible for it must take the necessary steps to ensure that continued compliance with the University's obligations under the DPA 1998 can be demonstrated. In particular:

- data subjects, University employees and 3rd parties permitted to access the personal data should all be regularly reminded of their rights and obligations
- all proposed future changes to the system, both technical and administrative, should be reviewed for their data protection implications prior to their implementation, and where necessary, advice on their impact should be sought from the University's Governance Officer (Data Protection and Legal), including on whether a Privacy Impact Assessment is required

9.5.3 Turnitin and GradeMark

The University has subscribed to Turnitin®UK, a text-matching software service that may be used to assess the originality of student work or alternatively, may be used by students to submit their own written work. GradeMark is an essay marking tool provided by Turnitin. Information about these services, their use at the University and their data protection implications is available:

for staff at: http://www2.napier.ac.uk/ed/plagiarism/staff-TurnitinUK.htm

or students at: http://www2.napier.ac.uk/ed/plagiarism/students.htm

9.5.4 Developing an e-learning system

When developing an e-learning system, ensuring best practice compliance with data protection law should always be built into the planning and design process. Staff involved in any such development should seek advice from the University's Governance Officer (Data Protection and Legal) and consider whether a Privacy Impact Assessment is required. Factors which must be considered are:

- proposed uses of personal data
- the potential 3rd parties from whom transfers of personal data may be received into the system, or to whom data may be transferred from the system
- the respective data protection risks and the University's responses to these

Further discussion and advice on ePortfolios, VLEs and data protection can be found at: http://www.jisc.ac.uk/uploaded_documents/Data_Protection_FAQ.pdf and in this JISC checklist.

10. PRIVACY IMPACT ASSESSMENTS

10.1 General

Where University staff are considering adopting new administrative systems and other processes with possible privacy implications, or updating existing systems or processes (such as student record systems, virtual learning environments (VLEs), ePortfolio systems and distance learning programmes) they should consider undertaking a Privacy Impact Assessment (PIA) in the early stages of project or process design, well before roll-out/implementation.

10.2 Privacy Impact Assessment is defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders and a constructive search is undertaken for ways to avoid, minimise or at least improve privacy concerns. PIAs are most effective when they are:

- Applied to initiatives under development, at a time when the personal information aspects are known, but before key development, system design, and operational decisions are set in stone and become costly to change
- Part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes, as is common with other forms of threat/risk assessment

10.2 Guidance

There is further Guidance on PIAs, including advice on when a PIA should be carried out, who should be involved and what form the process might take. A Template PIA form is also available.

The UK Information Commissioner has published a Privacy Assessment Handbook.

11. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Under the DPA 1998, there are different legal requirements for contracts depending on which country the data will be held in. The most important distinctions are whether information will be held:

- within the EEA
- by a country on the European Commission's approved list; or
- in another non-EEA country.

11.1 Transfers of Personal Data to European Economic Area (EEA) Countries

The countries which constitute the EEA are the 27 members of the European Union, together with Lichtenstein, Norway and Iceland. The full list is available at: http://europa.eu/abc/european_countries/index_en.htm

These countries are considered to ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This means that transfers of personal data between those countries are automatically permitted.

However it is unwise to assume that transfers of personal data to, or from, other EEA States will always be straightforward. Prior to beginning any personal data transfers to EEA States, University staff should:

- Evaluate the relevant national legal and administrative compliance criteria for personal data transfers in all countries involved
- Liaise with appropriate officers in institutions/organisations to, or from, whom data is to be transferred, to allocate responsibility for ensuring that appropriate legal and administrative formalities have been satisfied
- Document both the legal and administrative requirements, and the agreed responsibilities of the respective parties, ideally in a contractual document, with appropriate warranties and indemnities in case of breach

Template clauses to incorporate into an existing agreement and a separate standalone template agreement are available from the Governance Officer (Data Protection & Legal).

11.2 EU Commission Approved List

11.2.1 Some countries outside the EEA have been officially deemed by the EU Commission to have an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The EU Commission publishes a full list of approved countries, which includes Argentina, Canada, Switzerland, Guernsey and the Isle of Man.

11.2.2 There is a partial finding of adequacy for the United States with regard to those organisations who have volunteered to be subject to the US/EU Safe Harbor principles.

11.2.2 Where the country has been formally assessed as providing adequate protections, the transfer is to be treated as a data transfer to an EEA country and the template clauses and agreements referred to in 11.1 above are to be used.

11.3 Transfers of Personal Data to Non-EEA Countries

The DPA 1998 contains specific provisions with regard to the transfer of personal data to countries outside the EEA. The eighth data protection principle states "'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." This is qualified by a number of conditions e.g. personal data may be transferred to a country without an adequate level of protection where the data subject has given consent to the transfer.

11.3.1 University staff should ensure that there are clear and documented procedures and administrative responsibilities for the transfer of personal data to non-EEA countries. University staff should consult this checklist when considering if a transfer of personal data is proposed.

11.4 Exceptions to Prohibition on Data Transfer

The DPA 1998 provides a number of exceptions to the prohibition on the transfer of the personal data in question, details of which are given with the checklist above.

11.4.1 Use of exceptions

Any use of these exceptions must be fully documented in order to justify the basis for any transfer made to a third country, in case of a challenge made by either the ICO or in the courts.

11.5 Consent

The potential benefits of obtaining specific and informed consent of data subjects before the transfer of data to a non-EEA country are:

- The data subject can be made aware of the risks that the University may have assessed as being involved in the transfer; and
- The data subject is able to give their clear and unambiguous consent to the transfer

Examples would include the transfer of staff personal data to a non-EEA country to be used in the management of a distance learning course and where a data subject requests a reference be written and sent to a non-EEA country. In the latter case the request itself will indicate consent to the personal data transfer.

Staff involved in any transfers where consent is relied upon as the justification for the data transfer must ensure that they:

- document that the data subject was informed as required
- obtain consent in writing, unless there are suitable technological means to ensure that authenticated consent can be collected on-line
- retain evidence of both the above

11.6 Method of Transferring Personal Data

Where it has been established that personal data may be transferred, this should be done in accordance with section 7.5 of this Code of Practice; electronic transfers of personal data must be encrypted. IT Services provide guidance on both Data Encryption and on Email Encryption

11.7 Third Party Requests

University staff must ensure that personal data is not disclosed without the specific and informed consent of the data subjects concerned when requested by:

- non-EEA governments, agencies, and organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas where there is no sponsorship arrangement or other agreement between the data subject and a third party
- non-EEA governments for the purposes of determining liability to attend National Service

11.8 Data Controller Assessment of Adequacy for Non-EEA Transfer

Where none of the above options apply for a transfer outwith the EEA, the University may determine that the transfer it wishes to make will provide adequate safeguards.

However this must be discussed at the outset with the University's Governance Officer (Data Protection and Legal) who will seek any necessary legal advice and ensure that the relevant area conducts a risk assessment.

11.9 Further Information on International Transfers

The UK Information Commissioner has provided the following guidance:

- **General advice on the eighth data protection principle:** http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#international

- **General advice on how to comply with the eighth data protection principle:** http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/generic_guidance_int_transfers_v3.pdf

12. COLLECTION & PROCESSING OF PERSONAL DATA RELATING TO DISABILITY

12.1 General

Key areas for which the University needs to collect and process sensitive data is in service provision for disabled employees and students and mandatory monitoring and reporting. The University collects student disability information at the admission stage e.g. through UCAS, reference letters and interviews and employee disability information at interview stage. However, collection of disability data may also occur throughout the period of study or employment. University procedures are in place to protect an individual's privacy and permit necessary disclosure.

12.2 Disclosure by Individuals

12.2.1 There is a close correlation between disclosure of disability status and the University's ability to ensure that as full a range of support services as possible can be supplied, in order to make any reasonable adjustments as required by the Equality Act. We also need to demonstrate that we monitor this data to ensure that our equal and diversity policies are working.

12.2.2 The University therefore encourages staff and students to provide this information when requested. It will then be processed in accordance with the DPA 1998, this Code of Practice, and the University's Data Protection statements for staff and students. The data will only be made available to those people who strictly need to know for the purposes of e.g. employment, teaching, examinations, or domestic facilities, including student residential accommodation, to implement any relevant reasonable adjustments. In many cases it may be sufficient simply to tell another member of staff what adjustments are required to assist a staff member or student, without explaining the nature of their disability.

12.3 Seeking and Giving Consent

Explicit consent from the individual is normally required when processing sensitive personal data, including disability. This means that on every occasion and before consent is sought, the individual must be informed about the nature of the information to be disclosed, the intended recipient and the purpose for the disclosure. The means by which the disclosure will be made e.g. password protected or encrypted email must also be considered.

Blanket, or wide-ranging definitions of purpose on consent forms are therefore inappropriate and the use of an opt-out must not be relied on to cover the transfer of such data. The template consent form for the disclosure of sensitive personal data should be used for this purpose.

12.4 Where Consent is Withheld

Although members of staff need to take steps to find out if a student or staff member is disabled in order to put reasonable adjustments in place, a disabled person may request that the existence or nature of his or her disability is treated as confidential. The University cannot guarantee that in every case such a request will be adhered to since this will depend on the circumstances. As at 12.2.2 above, in some cases this can be overcome by advising what the reasonable adjustments are but in others the disabled person must be advised that this may adversely affect them where the University is not allowed to disclose the information.

12.5 Disclosure in Exceptional Circumstances

The University's procedure for the disclosure without consent, of sensitive information which may have been given in confidence, is referred to at section 8. of this Code. The provisions of the Equality Act do not override the Data Protection Act or Health and Safety legislation. If there is a genuine overriding health and safety risk, or there are issues about duty of care to a student or member of staff then it may be appropriate to make a disclosure without consent in exceptional circumstances, e.g. where there is:

- a serious risk to the health and safety of an employee or student
- a risk of serious abuse or exploitation
- behaviour which is seriously affecting others
- a possibility that a criminal or serious disciplinary offence has been committed
- serious concern that a student's health or behaviour may compromise the University's responsibilities to outside agencies, such as partner institutions or practice placements.

The procedure for any such disclosure is given in Section 8.5

12.6 Disclosure in References

These are dealt with in Section 19.4 of this Code of Practice.

12.7 Disclosure to Third Parties

Where it is necessary to disclose sensitive personal data e.g. details of a disability to a third party this should be done strictly in accordance with this Code of Practice, Section 7: Security of Personal Data and Section 8: Data Sharing.

12.8 Further Information

Further information on equality and diversity is available for staff and students.

13. NEXT OF KIN & EMERGENCY CONTACT INFORMATION

University staff and students are asked to provide details of their next of kin and emergency contacts. Those nominated persons will only be contacted for emergency purposes in the immediate health or safety interests of a staff member or student. Staff and students must ensure these details are kept up to date and that they have told the individual or individuals to be contacted, of the disclosure to the University of their details.

Staff should review their contact details on an annual basis through HR Connect Employee Self Service .

Students may change these and other personal details at any time by logging onto the Student Records system, Nimweb

14. COUNSELLING SERVICES

The University provides in-house counselling services for students and an independent service from Care First for staff.

14.1 Counselling for Staff

Staff should visit the Care First website.

The Student Counselling Service also offers advice to staff on referring students to them.

14.2 Counselling Service for Students

The University has a counselling service for students and legitimately collects and processes personal data, including sensitive personal data strictly in accordance with the Act and associated legislation. Guidance is available on the Counselling Service's procedures for:

- Data protection and confidentiality
- Access to counsellor's notes and other records; and
- Records retention

15. STUDENT ADVICE

15.1 Student Development

The University's Student Careers and Mentoring Service legitimately collects and processes personal data, including sensitive personal data in the course of its ordinary business, strictly in accordance with the DPA 1998.

The Student Development website contains comprehensive guidance on the services offered to students. The University is legally obliged by the Higher Education Statistics Agency (HESA) to collect first destination data for graduating students and the University's Careers and Mentoring Service undertakes this task. Disclosures to HESA are referred to in the Data Protection Statement for Students and in the HESA Information for Students.

All other uses of the data internal or external to an institution should be in the form of anonymised data unless the consent of the data subject has been obtained in advance.

15.2 Applications for Access Funding & Other Discretionary Funding

15.2.1 Students may be allocated funds from money given to HE institutions by the Scottish Awards Agency for Scotland (SAAS) on behalf of the Scottish Government for the provision of the Discretionary Fund and Childcare Fund. Students will normally be invited to apply for help and complete an application form and the data provided will be processed strictly in accordance with the DPA 1998.

15.2.2 Decisions on whether to allocate funds to individual students are made on the contents of their application form and/or on the basis of confidential documents provided by the students. Students are entitled to have access to any personal data held by the University with regard to an application for Discretionary and Childcare funding, unless the data cannot be disclosed without additionally disclosing personal data about a third party. These criteria should also apply to any other funds administered by Student Development and Wellbeing within Student and Academic Services

15.3 Napier Students' Association

Napier Students' Association (NSA) is a separate organisation and is not covered by the University's Data Protection Notification to the UK Information Commissioner. Procedures are in place therefore to assist NSA staff to work with the University to support the ongoing academic and pastoral welfare of students. NSA Advisers will ask students to complete disclosure forms at their first interview and a copy of this form should be provided to staff members on request to ensure that there are no inappropriate disclosures.

The link to the website for NSA is: www.napierstudents.com

16. CCTV AND SIMILAR SURVEILLANCE EQUIPMENT

The University uses CCTV across its campuses to ensure site security and the safety of staff, students and visitors. Since these systems invariably require the processing of personal data, their use must comply with the DPA 1998. In accordance with guidance from the UK Information Commissioner, the University has adopted a Code of Practice for the use of CCTV.

17. PHOTOGRAPHY AND FILM

Photographs and other digital images of identifiable living individuals are personal data and therefore subject to the principles of the Act, except where photographs are being taken strictly for personal use.

17.1 Consent

Where consent is required this must be freely given at the time the image is taken and only after the subject has been informed of the specific purposes for which their image will be used. Guidance on the different methods of obtaining consent will depend on the type of image to be taken and any limitations on its use. The relevant consent forms are available at 17.10 below.

17.2 Publication on the internet

This means that images will be available worldwide. In view of the very widespread nature of the disclosure and the effect upon the privacy of the individual, consent for publishing photographs on the internet is required from the subject. It is important to be aware that consent will not be considered as valid by the UK Information Commissioner unless it has been clearly explained to the individual that their images will be available throughout the world, including in countries outwith the European Economic Area (EEA) where their rights are not protected by UK law.

17.3 Crowd/General photographs

If photographs are to be taken of a crowd of people, consent does not need to be obtained if none of the members of that crowd can be readily identified from the photograph. By choosing angles carefully it is possible to avoid recognisable individuals e.g. by using low angles, backs of heads, blurred or out of focus images. If any one person should become the focus of a crowd scene then where appropriate and feasible they should be asked for their consent in writing. If this cannot be obtained or is not given and measures are not taken to make the individual unidentifiable, the photograph should be deleted immediately.

17.4 Large group photographs

Where photographs are to be taken of a large group e.g. a lecture then this should be announced in advance so that individuals may leave the venue briefly if they do not wish to appear in the photographs.

17.5 Smaller group photographs

When a smaller group of people is to be photographed e.g. those attending a seminar, then the participants should be given the option of leaving briefly as in 16.2.4 above or the informed consent of each member of that group should be obtained. Where it is not practical to do this verbal consent should be sought.

17.6 Individual photographs

Informed written consent must be obtained when taking photographs of a specific person. This must includes all forms of intended use of the images including publication on the world wide web, in multimedia presentations or printed material.

If the photograph is to be used at a later date for a purpose which has not previously been specified, consent must be obtained from the individual for this new purpose.

17.7 Subjects under the age of 18

Please note that consent for photographs of subjects under the age of 18 must normally be sought from and given by a parent or guardian.

17.8 Event photography

Where a University event is being organised at which photographs are to be taken by in-house photographers or an external agency, there are some measures which should be taken to ensure that individuals are aware that photographs will be taken and the reasons for this. These include:

- if tickets are being issued this information can be printed clearly on the reverse
- a pro forma display notice should be prominently displayed
- a reference to photography could be included in any online announcements or programmes to be used at the event

Wherever practicable and appropriate it should be considered whether consent is to be sought. Where external agencies are employed they should be informed of the University's policy and given a copy of this Guidance. There is also a checklist which should be used for any special or unusual events.

17.9 Storing the images and forms

Images and any associated forms must be kept securely whether in electronic or manual format in accordance with the DPA 1998 and the University's Information Security Policy and Manual Data Security Policy.

In addition, since the University must be able to comply with an individual's right to access their personal data, those taking photographs must ensure that any such requests can be dealt with promptly. The University's photographers have created a central database for this purpose and all those taking photographs on behalf of the University should send to them by the most secure method a completed copy of the consent forms together with a disk of any photographs, so that they may be catalogued and stored securely.

17.10 Consent forms and Further Information and Guidance

These are available from the University photographers

18. EXAMINATIONS AND ASSESSMENT PROCESS

All personal data produced and processed for the purpose of examinations and assessment will be subject to a student's right of access under the DPA 1998, except where an exemption applies.

18.1 Examination scripts

Examination scripts are expressly exempted from the data subject's right of access. This means that the University is under no obligation to permit examination candidates

to have access to either original scripts or copies of those scripts. Examination means any process for determining the knowledge intelligence skill or ability of a candidate by reference to his performance in any test work or other activity, thus written assessment work and field work are covered. However this exemption is discretionary and the University may still choose to provide a script under a subject access request.

18.2 Examiners' comments

Both internal and external examiners' comments, whether made on the script, or in another form that allows them to be held and applied to the original script (e.g. in a coded table), will be covered by the DPA 1998. A data subject has the right to request that a copy or summary "in intelligible form" is provided within the stipulated timescale. This limit is normally 40 days, but in the case of examinations the Act specifically notes that a request may be made before results are announced. In this case there is a limit of five months from the request or 40 days from the announcement of the result, whichever is the earlier.

18.3 Examination marks

The DPA 1998 provides an exemption in relation to the period in which the University is required to deal with a request for access to examination marks, if that request is made before the results are published. The University must respond within five months of the date of the request or 40 days of the date the results are published, whichever is the earlier.

18.4 Providing feedback

Provision of feedback on both formative and summative assessment is increasingly seen as an important part of the educational process to promote learning and facilitate improvement. In order to provide feedback "in intelligible form" academic areas must ensure that examiners write comments that are readily comprehensible, in the absence of the script, to reduce the likelihood that the University will only be able to meet this requirement by producing the script.

18.5 Automatic processing

The DPA 1998 provides data subjects with the specific right to be informed of the logic of any purely automated decision that significantly affects them. The University's Faculty and School examination boards review and validate the results of each student, taking into account such variables as personal circumstances and health issues.

18.6 Examination Board minutes and related documentation

Minutes of i) the University's Examination Boards that contain discussion about data subjects; and ii) the University's Faculty Extenuating Circumstances Boards which are prepared for the purposes of supplying recommendations for consideration by Examination Boards, will be subject to data subject access where candidates are named, or referred to by identifiers from which students may be identified (e.g. by matriculation number) and an extract of the relevant entry (entries) will be provided.

It should be noted that examination board minutes and related documentation which concerns general discussions, e.g. about moderation standards, will very likely be accessible to individuals under the Freedom of Information (Scotland) Act 2002, (FOISA) unless an exemption can be claimed.

To comply with the University's obligations under both DPA and FOISA legislation, clerks to the Examination Boards should ensure that the minutes of meetings are prepared so that the recording of discussions about specific students is kept separate from that of general business matters. A FOISA front sheet has been developed for this purpose.

18.7 Disclosure of results

Since examination results constitute personal data they should not be disclosed to third parties unless one of the relevant criteria in the DPA 1998 is met. The usual criterion is to gain consent to the disclosure e.g. for inclusion of results in the graduation lists published in "The Scotsman" newspaper and in the Graduation Programme. If a student has opted out of publication, staff must not then disclose results to enquirers, unless specifically requested to do so by the data subject in writing, or where there is legitimate reason to do so, such as the prevention of fraud, e.g. where a student misrepresents their results to an employer. The University's procedure for dealing with false qualification claims is in Section 8.10 of this Code of Practice.

18.8 Withholding results

Results will be withheld in accordance with the University's policy on Tuition Fees (which includes provisions governing other student debt) and the University's obligations under the DPA 1998.

19. REFERENCES

The two principal aims of a reference are to provide facts and opinions as to a candidate's suitability and therefore this necessarily involves not only data protection but also legal implications in the provision and receipt of references. Detailed guidance on these is available in the University's Guidance Note on References

19.1 References given by the University

References given by the University, including, references written by employees in their formal capacity, or as part of a standard procedure, (e.g. as Head of Department, as part of a promotions exercise) are exempt from subject access requests where those references relate to:

- Education, training or employment of the data subject
- Appointment of the data subject to any office
- Provision by the data subject of any service

The University has the absolute discretion to refuse to release references written on its behalf if requested to do so in, or as part of, a subject access request. However, the fact that the exemption is discretionary means that the University may still choose to provide references written on its behalf under a subject access request.

19.2 References received by the University

19.2.1 References received by the University are not exempt from the right of access, but consideration must be given to the data privacy rights of the referee. Information contained in, or about, a reference need not be provided in

response to a subject access request if the release of this information would identify an individual referee unless:

- The identity of the referee can be protected by anonymising the information
- This referee has given his/her consent, or
- It is reasonable in all the circumstances to release the information without consent

19.2.2 In considering whether it is reasonable in all the circumstances to comply with a request, the ICO suggests that the account should be taken of factors such as:

- Whether the referee was given express assurances of confidentiality
- Any relevant reasons the referee gives for withholding consent
- The potential or actual effect of the reference on the individual
- The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- That good employment practice suggests that an employee should have already been advised of any weaknesses; and
- Any risk to the referee

In cases where a reference discloses the identity of an organisation, but not an identifiable individual, as referee, disclosure will not breach data privacy rights.

19.3 Internal references

There may be circumstances where a reference is written on behalf of a data subject by an individual in one department of the University, to be used by an individual in the same or another department of the University. It should be noted that the ICO considers internal references to be 'management data' rather than references and that therefore disclosure may be required.

19.4 Disclosure of disability in a reference

Where an individual refuses to consent to disclosure of a disability in a reference, the referee must decide if they can write a reference under those circumstances, reflecting their duty of care to both the individual and the person or organisation requesting the reference. If a referee feels that they cannot meet their duty of care to either party under those circumstances, they should inform the individual that they will be unable to write a complete reference without referring to the disability, and that this would not be in the best interests of either the individual, the person or organisation requesting the reference, or the University which is providing the reference. If consent is still unforthcoming, no reference should be written.

20. RETENTION OF RECORDS CONTAINING PERSONAL DATA

There has been considerable development in records management in recent years, which has been driven not only by the statutory requirements of the DPA 1998, the Freedom of Information (Scotland) Act (FOISA) and the Environmental Information Regulations 2004 (EIRs), but also by the data retention requirements of the legislative and regulatory framework, within which HE institutions operate.

20.1 Records Retention under the Data Protection Act 1998

The DPA 1998 requires that personal data is kept only for as long as is necessary. The relevant retention period for individual classes of data are determined by statutory requirements, professional requirements or best practice.

20.2 University and JISC Retention Schedules

All staff must be aware of their obligations for the appropriate retention of records containing personal data. The University's Records Management Unit is actively developing retention schedules

Staff are also advised to refer to JISC's Business Classification Scheme (BCS) and Records Retention Schedules (RRS) for Further and Higher Education Institutions at: www.jiscinfonet.ac.uk/projects/records-retention-fe/index_html and:

www.jiscinfonet.ac.uk/partnerships/records-retention-he

and, in particular, the Records Retention Schedules at: www.jiscinfonet.ac.uk/projects/records-retention-fe/database-status and:

www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-rrs

20.3 Destruction of Records Containing Personal Data

Once it has been established that records containing personal data may be destroyed, this must be done in accordance with the University's guidance on the Safe Disposal of Confidential Waste.

20.4 Record of Destruction

In order to ensure that the University will be able to demonstrate its legislative compliance in the event of a request under the DPA, (or FOI(S) A, EIRs) being received, a record of the data which has been destroyed and the basis on which this was done (e.g. in accordance with a legal requirement) must be kept for five years by the area in which the destruction took place. The University's Record Disposal form should be used for this purpose.

21. GLOSSARY AND ACRONYMS

CCTV	Closed Circuit Television
DPA 1998	UK Data Protection Act 1998.
DPD 1995	EU Data Protection Directive 1995 (Council Directive 95/46/EC, 1995 OJ (L 281) 31-50.)
Direct marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals'. (DPA 1998 s.11)
ePortfolio	A collection of electronic evidence assembled and managed by a user as a learning record that provides actual evidence of achievement.
EEA	European Economic Area - the 27 EU Member States, plus Iceland, Liechtenstein and Norway.
EU	European Union - Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.
FOI	Freedom of Information
FOISA 2002	Freedom of Information (Scotland) Act 2002. This covers public bodies over which the Scottish Parliament, rather than United Kingdom Parliament, has jurisdiction
FPS	Fax Preference Service
HE	Higher Education
HESA	Higher Education Statistics Agency
HRA 1998	Human Rights Act 1998
ICO	Information Commissioner's Office
LBPR 2000	Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
PEC Regs	UK Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended 2011
PIA	Privacy Impact Assessment
RIPA 2000	Regulation of Investigatory Powers Act 2000
SMS	Short Messaging Service (text messaging)
TPS	Telephone Preference Service
VLE	Virtual learning environment