EXTRACT FROM DATA PROTECTION CODE OF PRACTICE

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 FOISA, 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 some important changes were made, which included:

- rules for websites using cookies and similar technologies (see section 9 of this Code of Practice);
- 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
- new powers for the ICO to investigate breaches of the Regulations by obtaining information from certain third party organisations.

Most of the rules on marketing by live phone call, automated phone call, fax, email and text message stayed the same.

'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.

The ICO has published this updated ‘plain language’ guidance on PECRs.

Enforcement of PECRs

The Privacy and Electronic Communications Regulations are enforced by the ICO, who may 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.