EXTRACT FROM DATA PROTECTION 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, 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”

Central guidance has been developed to explain to relevant University staff what they must do to comply with the new regulations on cookies referred to in 9.2.2 above.

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 Governance Services.

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 and cloud computing 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 Governance Services.

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 Legal has prepared a "Tutor's Checklist for Staff", which is included at Appendix A.

9.5 Cloud Computing Services

The UK Information Commissioner (ICO) has published guidance on cloud computing services which includes this definition: 'cloud computing services offer organisations access to a range of technologies and service models typically delivered over the internet'. In the accompanying overview, the ICO states:

'Organisations that maintain and manage their own computer infrastructure may be considering a move to cloud computing to take advantage of a range of benefits that may be achieved such as increased security, reliability and resilience for a potentially lower cost.

By processing data in the cloud an organisation may encounter risks to data protection that they were previously unaware of. It is important that data controllers take time to understand the data protection risks that cloud computing presents'.

The University's IT Services offer a range of internally hosted cloud services which staff and students must consider first before then investigating the transfer of personal data (or confidential/ commercially sensitive University information) to an externally hosted service. If it is agreed that the University is unable to provide what is required, any staff member intending to use an external service must:

- Refer to the ICO's guidance and in particular the checklist at s.98 which covers these headings: 'Risks, Confidentiality, Integrity, Availability & Legal'
- Consider and where necessary seek legal advice on the terms of the agreement with the cloud provider
- Ensure they can demonstrate that they can satisfy the legal requirements of signing up to the service
- Seek the written approval of their line manager
- Consult Governance Services

9.6 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 is available on the Moodle Student Help pages.

9.6.1 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.

9.6.2 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 Governance Services, including on whether a Privacy Impact Assessment is required

9.6.3 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

9.6.4 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 Governance Services and complete a Privacy Impact Assessment. 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.