Queen's University Belfast

Security Policy 06 - INFORMATION HANDLING POLICY

OBJECTIVE

The objective of the **Information Handling Policy** is to ensure that effective measures are in place for the protection of the University's **information assets**.

Notes

1 *Information assets include databases and data files, system documentation, user manuals, operational and support procedures, continuity plans and archived information.*

2 *Users should be familiar with the University's Data Protection Regulations – see http://www.qub.ac.uk/dataprot/webpages/university_policy.htm*

3 *See http://www.qub.ac.uk/is/StaffComputing/ITServices/SecurityandAnti-Virus/SecurityPolicies/*

4 *An inventory template is attached to this policy*

POLICY

- Directorates and Schools are best placed to understand their **information assets**[1] and the need to protect them against loss or unauthorised access. The purpose of this Policy is to set out clear minimum standards to assist departments in the usage, storage and transfer of sensitive data which falls within their areas of responsibility.
- The **Data Protection Act**[2] requires that appropriate measures (technical and organisational) must be taken against unauthorised or unlawful access to personal data and against accidental loss or destruction of personal data. In addition, the University has valuable commercial and research data that must be protected.
- The **security of information** in the possession of the University is of paramount importance and is addressed in various **policies and procedures**[3] throughout the institution. The University's **Records Management Policy** also gives guidance on the systematic management of records within the University to ensure that valuable business information and evidence of business activities are controlled and maintained.
- Directorates and Schools must maintain an **inventory**[4] of the information assets for which they are responsible and must ensure appropriate protection of those assets. As part of that, they should identify a named **information owner** who has lead responsibility for that information, including how it is managed and shared. They should also identify the particular **sensitivity** associated with the information, as this will inform decisions on how the information should be handled. Examples of sensitive information include:
  - Personal data (e.g. staff or student personal details, salary details)
  - Sensitive financial information (e.g. the value of contracts, at least at certain points)
  - Confidential information (e.g. exam scripts or marks, internal reports)
  - Research information of commercial or other value to the University, which the University does not want to share.
  - Sensitive information about others which might be given by third parties for research purposes (e.g. patient data) which would cause harm or distress if released.

- Information owners must ensure (either directly or through Information Services) that appropriate mechanisms are in place to **protect**[5] information assets for which they are responsible. If there is any doubt whatsoever about the appropriate mechanisms to use then advice should be sought from Information Services before proceeding.

- Any **breach of security** involving sensitive information must be reported immediately to Information Services.

- The **University website should not be used to store or make available sensitive information**, even where the pages or intranet sub-sites containing the information have been password-protected. If you need to make sensitive information available online then **Sharepoint** is the recommended tool. Even then, issues such as access and retention need careful consideration.

- The University advocates a **clear desk and screen policy** particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

- Sensitive data or information may only be **transferred**[6] across networks (including email) or copied to other media when the confidentiality of the data or information can be assured throughout the transfer. Where appropriate, data encryption should be used. Please see SP07 and SP-UG1 for policy and guidance.

- Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must be seen to continue to **assure the confidentiality and integrity of the information**[7].

- **Removal**[8] off-site of the University's information assets, whether on paper or on laptops or other mobile storage devices (USB pens, CDs, etc.), must be properly authorised by the responsible information owner. Prior to authorisation a **risk assessment**[9] should be carried out and appropriate risk management processes put in place.

- Third party organisations from which the University receives sensitive data (e.g. NHS Trusts) may have their own policies regarding the handling and processing of such data. Staff and students must ensure that they comply with the relevant policies before handling or processing data belonging to such organisations.

- All users of University information systems must manage the creation, storage, amendment, copying and deletion or destruction of data (in electronic and paper form) in a manner which is consistent with the policy set out above, and which safeguards and protects the confidentiality, integrity and availability of such data.

- This policy should be read in conjunction with the University's Regulations and Statements of Best Practice relating to:-
  - Data Protection
  - Mobile Computing

- Changes to this policy in response to changing demand, both operational and legislative, will be available on the University WWW site.

5 *This includes but is not limited to:*
- *The security and integrity of information assets*
- *Backup and system recovery*
- *Disposal of printed material and storage devices*
- *Archival of information assets*

6 *Where necessary, advice should be sought from Information Services or School-based Computing Officers on appropriate mechanisms for the secure transfer of sensitive information, particularly outside of the University's secure environment.*

7 *A written agreement, setting out the responsibilities for proper handling of the information, should be agreed in advance. A formal Data Processing Agreement is required under the Data Protection Act for the processing of personal data by third parties.*

8 *The University has a separate policy for mobile computing and this must be adhered to in all situations where sensitive information is removed from the University.*

9 *A risk assessment template is attached to this policy*

School / Directorate	

Description of Information Asset	**Information Owner**	**Sensitivity (e.g. Personal Data; Sensitive Financial Information)**

Information Asset		**Information Owner**	
Description of Information Handling Requirement			

Description of Risk	**Impact** **1. Minor** **2. Moderate** **3. Significant**		**Likelihood** **1. Low** **2. Moderate** **3. High** **4. Very High**		**Impact * Likelihood**		**Action to reduce risk**	**Respon-sibility**
	Gross	Net	Gross	Net	Gross	Net		