University of Glasgow

Policy on Confidential Data in the University

Information Security Advisory Group

Version 3.0

November 2010

Introduction

Much of the information or data that we handle as part of our daily work is not confidential and poses few if any real security concerns, aside from the inconvenience of it becoming unavailable. A proportion of the data concerns people, commercial activities, security or operational matters that need to remain confidential to a limited number of people. A number of high visibility incidents have occurred in other organisations over the past year or two, where data that should have remained confidential have been mislaid, stolen or leaked. Some such incidents (although not all) could have very serious consequences and it is important that this possibility is taken seriously and that an assessment of the risk is undertaken when confidential data is stored on computers, other devices, CDs and memory sticks and when such data is transmitted from one place to another. Such an assessment allows appropriate measures to be put in place to reduce the likelihood and/or impact of things going wrong.

Confidential data may arise in administration, teaching or research and may be concerned only with activities internal to the University or may involve outside bodies such as government departments, commercial organisations or the NHS. In this latter case, the NHS has recently issued '*NHSScotland Mobile Data Protection Standard v1.0*' (29 September 2008) which addresses the handling of confidential information relating to patients and is clearly directly applicable to those in the University handling such information.

It is clear that similar concerns and controls will apply more widely to any confidential data, such as that:

- relating to living individuals,
- given in confidence,
- subject to specific constraints or,
- relating to security,

that is generated by research, teaching or administration right across the University (see Appendix 1 for detailed definitions). With regard to external data, it is clear that the University has a responsibility to mirror the arrangements and policies of external bodies, not only in relation to mobile devices but wherever and whenever confidential data are stored in the University. If external data are also Personal Data they should also be covered by a data processor agreement in which the obligations on the University and any liabilities should be clearly outlined.

From April 2010, the Information Commissioner has the power to levy fines on an organisation of up to £0.5M "*if a data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress*". The Statutory Guidance issued provides a number of examples of cases that might lead to significant fines:

> ***Serious contravention example*** *- The failure by a data controller to take adequate security measures (use of encrypted files and devices, operational procedures, guidance etc.) resulting in the loss of a compact disc holding personal data.*

Damage example *- Following a security breach by a data controller financial data is lost and an individual becomes the victim of identity fraud.*

Distress example *- Following a security breach by a data controller medical details are stolen and an individual suffers worry and anxiety that his sensitive personal data will be made public even if his concerns do not materialise.*

Applicability and Implementation

This policy applies to all staff and students of the University. It applies to information belonging to the University or made available to an individual by virtue of their being a member of staff or student of the University, stored on whatever medium or device. The designers and maintainers of the major central information systems of the University will ensure that they operate their systems in accordance with this policy and it is the responsibility of University Services Departments, Colleges, Schools, Research Groups and individuals to ensure that their working practices conform to its requirements. This policy does not represent a fundamentally new requirement as much of it is implied by the Data Protection Act (1998) and reflects what recent rulings by the Information Commissioner have indicated is expected of organisations and individuals. The policy does not however confine itself to Personal Data (as defined by the Act) but extends the Act's principles to all information/data that might be the subject of confidentiality concerns.

Holding of confidential data in any form must be specifically authorised. Implementation of processes for this authorisation is devolved to Colleges and to University Services because the most appropriate way to manage this will vary across the University. The process needs to be tailored to the environment in which people work, so as to cause the least disruption. A central mechanism would not best meet the needs of different areas and would be too cumbersome if it had to take account of the specific needs of working with particular external bodies (such as the NHS, Professional Bodies, Local and National Government Departments, etc.). In some circumstances where an activity is carried out routinely in a number of places, a central mechanism may be appropriate (rather than specific authorisation). This is covered the document "Authorisation" which outlines the procedures and responsibilities for authorisation, under the heading "Generic Authorisations".

The policy itself lays down the basic principles for dealing with confidential data in the University. These are specified in broad terms only, so that they will remain stable through time. The detail of best practice guidance in relation to where to store information, what types of device to use and what technical measures are appropriate will change. Appendix 2 contains basic best practice guidance on using:

- central systems and desktop computers,
- laptop computers, other portable devices,
- memory sticks and other storage devices,
- data exchange both internally and externally,
- access to data

and the associated record keeping. This policy simply requires that current best practice is followed and the details of what this is will be maintained on a dedicated web site and to which Colleges, Schools and individuals should refer (**http://www.gla.ac.uk/confidentialdata/**).

Policy

Information that constitutes confidential data, (including NHS records) should not be stored, transmitted or processed on any University of Glasgow owned or managed computers, networks, servers, desktops, laptops or removable storage devices, or other machines or devices used by staff unless it is a part of a specific activity, project or system, authorised as indicated below.

Storage, use or transmission of confidential data as part of a specific activity or project should be authorised by a member of senior management in either the appropriate College or University Services (as designated by the College or Service). In relation to both external or internal research, this responsibility may lie with the College Ethics Committee, as part of its wider remit to oversee the ethics of research activity (but this is for the College to decide).

Authorisation to store, use or transmit confidential data should only be given after a clear indication of what is proposed has been articulated, a risk assessment has been carried out and the necessary steps to mitigate the risks identified, by those proposing or supervising the activity or project. This assessment must be sufficiently thorough to be acceptable to those responsible for its authorisation under this policy and should cover:-

- **an evaluation of what data are essential** for the specific activity, project or system;
- **the degree of sensitivity** of the data with respect to the extent to which it can be linked with individuals (directly or indirectly), the consequences of loss or unauthorised access and whether or not specific protection (as outlined in this policy and associated guidelines) is required;
- **the personnel that need to be authorised to have access** to the data in order for the work to be carried out;
- **the arrangements required for secure storage** of vulnerable data so as to prevent it being: accessed by unauthorised personnel, lost accidentally or stolen from University offices, from vehicles or from insecure premises.

Where a specific activity or project involving the use of confidential data is authorised, the authorisation process should specify what controls are required. These should take account of the risks involved and the Best Practice Guidelines issued from time to time by the University Information Security Advisory Group and available at: **http://www.gla.ac.uk/confidentialdata/**.

The mechanism for authorisation is the responsibility of the College or University Services where the activity, project or system is based. Committees or individuals charged with the responsiblity for authorisation of activities under this policy may wish to seek specific input from IT Services or the Data Protection and Freedom of Information Office in relation to the adequacy of the risk assessment and the appropriate arrangements for secure storage to reduce the likelihood of undesirable consequences.

Where confidential data are lost or stolen or where systems containing confidential data are compromised, this should be reported immediately to the College or University Service Management responsible for the authorisation of confidential data use, if computing technologies are involved, to the Computer Security Team and if it is information concerning individuals (as defined in the Data Protection Act 1998), to the Data Protection and Freedom of Information Office. In cases of theft or suspected theft the matter should also be reported to Campus Security who will involve the police if this is appropriate. Where the loss or compromise is likely to result in publicity, Corporate Communications should be briefed and kept informed as the situation develops, so that they are ready to deal with the media.

The aim of all parts of this policy is to ensure that the likelihood and impact of unauthorised access, loss or theft is minimised, thus protecting all the parties involved.

Explanatory Notes

We use the term ‘Confidential Data’ to include personal data, sensitive personal data, commercial in confidence data, and security or sensitive operational data. Much of this material might be expected to have an exemption from disclosure under the Freedom of Information (Scotland) Act 2002.

1) The Data Protection Act (1998) (and subsequent amendments) applies to any storage or processing of personal or sensitive personal data (specifically defined in the DPA 1998 as: "*obtaining, recording or holding…or carrying out any operation of set of operations… including organisation, adaption, alteration… retrieval, consultation or use… disclosure… alignment, combination, blocking, erasure or destruction.*".

2) Access to any confidential data should be available only to those who have a demonstrable need to access it. So that unless someone is a specifically named individual who has been granted the right to access the data, they should not be able to do so either accidentally or by design. In addition to named individuals this could be a group of staff or staff in a specific role (see the section "Generic Authorisations" in the "Authorisation" document).

3) Confidential data should only be on University machines when explicit authorisation for a specific activity or project involving those data has been obtained from the relevant College or University Services and, if the records originate in an external body (such as an NHS Board), by the relevant approval and authorisation processes of that body. It is for Colleges and University Services to put in place appropriate authorisation processes in their situation for data sets or systems as befits the circumstances.

4) If authorisation for storage of confidential data has been obtained, the records stored on University machines must be adequate, relevant and not excessive to meet the requirements of the specific activity or project, given that the impact of loss or accidental disclosure increases with data volume and comprehensiveness.

5) The risks of loss or accidental disclosure must be assessed by those proposing the collection, storage or use of confidential data and appropriate organisational and technical measures must be made for the safe storage and use of the data with particular attention paid to security and for their secure disposal or archiving when the specific activity or project comes to an end.

6) Confidential data, in whatever form and on whatever medium, taken or sent outside the University are particularly exposed to loss or accidental disclosure and must be appropriately protected, so that should it be lost or stolen they will not be accessible to unauthorised individuals.

7) Appropriate behavioural and procedural measures to provide a robust approach to managing the risk inherent in possession of confidential data are an important part of a data security policy. These should be used in conjunction with technical measures for physical security (including locks, filing cabinets, location of printers) and IT security (including access control and encryption). These measures taken as a whole are designed to prevent confidential data being: accessed by unauthorised personnel (for example by access to insecure computers or inadequate access control or by exposure via shared printers, insecure filing arrangement, etc.); lost accidentally (for example in a paper file, on a laptop or other mobile device or on removable media) or stolen from University offices, vehicles or insecure premises.

8) Authorisation of the storage and use of confidential data requires appropriate record-keeping detailing what has been authorised, the people involved, the risks that have been identified and the risk reduction measures that have been agreed in terms of both the procedural and behavioural framework and the technical measures required to secure the data. It is the responsibility of the College or Service to maintain these records and they are likely to be subject to audit, particularly if difficulties arise.

Appendix 1 - Definitions

Definitions of Confidential, Personal and Sensitive Personal Data

Necessary in order to ensure that this policy is understood in the same way by all those concerned.

What are Confidential Data?

In this policy, Confidential Data are defined quite broadly as a blanket term applying to any information that the University or individuals would not wish to come into the public domain. Such data come into a number of overlapping categories and includes:

- **data that relate to living individuals** or that could lead to the identification of a person referred to (directly or indirectly identifying information such as names, addresses, occupations, photographs);
- **data given in confidence** or data agreed or reasonably assumed to be kept confidential (secret) between two parties that is not in the public domain, e.g. information on business, income, health, medical details, opinion;
- **data subject to specific constraints** - such as ethical guidelines, legal requirements or research-specific consent agreements;
- **data which are concerned with security** or with other sensitive aspects of organisational operation.

In this policy 'Personal Data' is taken to mean data that are covered by the Data Protection Act 1998 and is therefore a sub-category of 'Confidential Data' and 'Sensitive Personal Data' is in the DPA 1998 a defined sub-category of 'Personal Data'.

Confidential also has a more specific meaning in relation to the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 (FOISA). FOISA defines it as "*information in respect of which a claim of confidentiality of communications could be maintained in legal proceedings…*" – there must be real grounds proving that the information was in contemplation of litigation, rather than just a chance. "*Information is exempt information if it was obtained…from another person …and its disclosure would constitute a breach of confidence actionable by that person…*". It cannot therefore be assumed that all data defined as confidential in the four bullet points above would count as confidential under FOISA and some of it may be discoverable by people looking for information under the terms of FOISA. If in any doubt guidance and assistance from DP & FOI Office should be sought.

What are Personal Data?

The Data Protection Act 1998 defines personal data as data which relate to a living individual who can be identified:

- from those data or
- from those data and other information which is in the possession of, or is likely to come into the possession of, those processing the data (e.g. researcher or administrator)

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

What are Sensitive Personal Data?

Sensitive personal data are defined in the Data Protection Act 1998 as data that include a person's race, ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sexual orientation, criminal proceedings or convictions or allegations of the commission of an offence.

Important: **Not All Data** obtained from research with participants may be confidential, personal or sensitive but NHS client related data (e.g. clinical data, records, letters and reports and medical research data of a similar nature) will be confidential and are likely to be personal and also sensitive.

Appendix 2 - Best Practice Recommendations

The Best Practice at the time of approval of the policy was simply a snapshot in relation to handling information in general and a requirement when it is of a confidential nature. Obviously as technology changes, the fine detail of Best Practice will change and the latest recommendations can always be found at:

http://www.gla.ac.uk/confidentialdata/