GUIDELINES 10

Classification of information held by UCL personnel, for security management purposes

Endorsed by the Chair of the Information Strategy Committee – 15 February 2011

1. Introduction

This guidance is intended to help you protect the electronic information for which you are responsible. It applies to all types of information, such as personal data or research, teaching, audit or financial information; some or all of these may be held on personal workstations, servers, shared drives, laptops, USB keys and mobile devices.

Most of us keep a wide range of documents, images, presentations, artwork, technical specifications or software on our computers, which require differing minimum levels of protection from disclosure or damage. This guide will help you categorise your information and then think about the most appropriate ways of storing it and protecting it against unauthorised access or use.

This classification relates to data for which you are responsible which may be held:-

- on devices and systems under your day to day management and custodianship.
- on servers or shared drives under the management of a database administrator or system custodian. In this case, you will need to liaise with the administrator(s)/custodian(s) about the sensitivity of your data; for example, there might be a need to set up separate servers/partitions with different levels of protection if the same server is being used for data of widely differing sensitivities.

This guide does *not* consider disclosure of information under legislation such as the Data Protection Act 1998 or the Freedom of Information Act 2000. Any requests under this legislation should be transferred immediately to the Records Office.

The classification considers information in terms of the degree of sensitivity rather than their purpose or format, and maps these to one of four levels of sensitivity: Secret, Highly Restricted, Restricted and Normal. The classification is neither exhaustive nor precise: it is provided as a guide to the way in which the different kinds of information are regarded by UCL, and you are asked to use your judgement in tailoring this to your specific data holdings and contexts.

For portable devices such as laptops, PDAs and USB keys, we hope that this guide will encourage you to think twice about whether you need to carry files of higher sensitivity around with you when you travel. NB take care when accessing your email from outside UCL as it is difficult to anticipate the content of emails sent to you.

1.1. How to use this guidance

The first step in protecting information is to focus on the risk of disclosure or loss and the resulting consequences. Appendix A to this guide explains a simple method of risk assessment leading to a suggested classification scheme which has been used to reach the classifications in Section 2. The information in Appendix A is not a comprehensive treatment of risk but is included to show how he classification table was created.

Because it can be quite time consuming to work out the risks associated with each of the many kinds of information you might hold, section 2 lists many groupings and types of information that staff often create and use. This includes personal data (see section 1.2); however, a lot of information that is not personal may also be confidential or needing of protection, for example contracts or legal, audit or financial information. This table should help you work out what types of information you keep and the security classifications that you should consider.

Once you have classified the data you hold (Appendix A and/or Section 2), section 3 provides security guidance on working out the most appropriate ways of protecting your information, including storage, access and everyday handling.

1.2. What is personal data?

Personal data is simply information about a living individual who can be identified from that information or other information held by UCL. It includes information held on all media and formats, such as computers, paper and audio-visual materials. The Data Protection Act 1998 provides rules for those who hold and use personal data.

1.3. Sources of advice and information

The Records Office - http://www.ucl.ac.uk/efd/recordsoffice/

- Records management
- Data protection
- Data holdings survey
- Register of research projects
- Freedom Of Information (FOI)

Computer Security Team - http://www.ucl.ac.uk/isd/common/cst

- Advice on encryption - http://www.ucl.ac.uk/isd/common/cst/good_practice/encrypt
- Advice on secure deletion - http://www.ucl.ac.uk/isd/common/cst/good_practice/secure_disposal_guidelines
- General good practice - http://www.ucl.ac.uk/isd/common/cst/good_practice

Information Security Policy & supporting policies - http://www.ucl.ac.uk/isd/common/cst/swg/policy

The NHS partners (information governance)

2. Classification

No.	Description	Secret	Highly Restricted	Restricted	Normal
1	**Information about named individuals**				
1.1	Documents containing personal descriptions of named personnel, given to you personally or to a closed set of recipients e.g. formal interview notes, disciplinary correspondence		O		
1.2	Documents containing financial or administrative information about named personnel, given to you personally or to a closed set of recipients e.g. staff salaries and grades, projections and costings, grant applications containing costed named posts		O		
1.3	Documents containing personal information about students or staff studying at UCL, held by you through a UCL educational or study administration role e.g. student profiles and logs, marks and assessments, examination submissions, interview and tutor notes, examination board minutes		O		
1.4	Documents describing a person's skills and capabilities, work performed, contributions to projects and tasks, held by you because of your roles within those projects and tasks e.g. work plans, time sheets, project progress reports			O	
1.5	Descriptions of individuals which are now public or widely disseminated e.g. biographical profiles, short CVs, personal web page content, blog profiles and entries, social computing materials (unless known to be from a malicious source), public domain address book information				O
1.6	Personal address books, containing information richer than is in the public domain			O	
1.7	Personal health data about identifiable individuals, held as documents, medical images, spreadsheets and/or databases	O			
1.8	Photographs: If the photographer has permission to take, store and publish a photograph, that will usually be enough to satisfy the Data Protection Act. Different protection will apply depending upon the kind of photograph and its intended purposes of use. Examples include staff/student face for identification, close up skin lesion with no identifying features, full body medical image, a child (for monitoring development), photos with permission for publication.	O	O	O	O
2	**Information about de-identified individuals**				

No.	Description	Secret	Highly Restricted	Restricted	Normal
2.1	Databases containing personal and/or health characteristics from which demographic characteristics and publicly used identifiers have been removed. Note: if multiple de-identified databases have been linked, the classification "secret" may be more appropriate.	O	O		
2.2	As 2.1, but that have also been checked to exclude patterns of trait that could be used to re-identify an individual			O	
2.3	Aggregate data sets that contain large numbers of characteristics and/or are based on small population numbers (note: an absolute number cannot be specified here: judgement will need to be exercised)			O	
2.4	Aggregate data sets that contain few characteristics and/or aggregate large population numbers				O
2.5	Summarised or masked information that is normally acceptable for inclusion in publications e.g. in academic papers				O
2.6	Manually de-identified clinical letters and reports, checked by an experienced person				O
3	**Information about named organisations and teams**				
3.1	Privileged disclosures and commercially sensitive material, not otherwise published by the organisation e.g. artefacts containing intellectual property disclosed under a non-disclosure agreement, draft reports shared for personal feedback by known colleagues, internal reports shared through bilateral collaborations		O		
3.2	Internal organisation reports and contributions to shared reports with UCL, shared with multiple parties but not widely disseminated e.g. contributions to project reports, deliverables, grant applications - which are about the organisation rather than having technical content		O		
3.3	Organisational information that is expected or permitted to be disclosed more widely but not public e.g. company profiles, advanced copies of press releases, contributions to teaching/research presentation material about an organisation			O	
3.4	Materials about the organisation that are known to be public or widely shared e.g. company annual reports, materials intended for web sites, teaching resources, conference presentations				O
3.5	Organisation or team activity reports, strategy, vision, collaborations that are not commercially sensitive			O	
4	**UCL corporate information (usually held in corporate systems but sometimes copied onto personally-managed devices)**				

No.	Description	Secret	Highly Restricted	Restricted	Normal
4.1	Student name			O	
4.2	Other student demographic details (e.g. address, date of birth, ethnicity)		O		
4.3	Student specific courses, modules and periods of study			O	
4.4	Student assessments (e.g. examination marks, progress reports)		O		
4.5	Student fees, bursaries, residence charges etc.		O		
4.6	Staff name, internal phone number, e-mail address				O
4.7	Other staff demographic details (e.g. address, private phone numbers, date of birth, ethnicity)		O		
4.8	Staff employment and contract details, increment date		O		
4.9	Staff salary details (e.g. salary, grade, discretionary awards)			O	
4.10	Staff financial details (e.g. bank account, tax code)	O			
4.11	Staff appraisals, promotions		O		
4.12	Staff assessments, disciplinary matters etc.		O		
4.13	Staff CVs			O	
4.14	Staff training records			O	
4.15	Estates and space details, departmental usage				O
4.16	Building records				O
4.17	Library records (excluding named-person borrowing records)				O
4.18	Research publications holdings				O
4.19	UCL Finance systems documentation, income and expenditure codes etc.				O
4.20	Research grant awards, budgets (excluding salary projections for named staff)				O
4.21	Research costing information that includes named person salaries		O		
4.22	UCL grant account transactions		O		
4.23	UCL policies and governance resources (excluding named party reports)				O
4.24	Committee minutes and accompanying documents			O	
4.25	UCL legal compliance reports		O		

No.	Description	Secret	Highly Restricted	Restricted	Normal
4.26	Internal and external audit results and reports		O		
5	**Resources containing technical domain information used for research, teaching and enabling activities**				
5.1	Confidential investigations and analyses performed by UCL at the request of third party organisations, through consultancy or service contracts	O			
5.2	Novel UCL research information, in interim forms expected to give rise to new published findings		O		
5.3	Resources containing technical domain information received from other parties under a formal NDA or in the spirit of non-disclosure e.g. software code, technical specifications, screen shots of pre-release applications, internal white papers		O		
5.4	Draft or interim materials or submissions provided by another party for peer review, feedback or evaluation e.g. draft academic paper, grant proposal, test version of software, pre-publication manuscript or artwork		O		
5.5	Resources containing technical domain information received from other parties on a personal basis, but intended for abstraction into more accessible forms e.g. raw data or detailed reports intended to be summarised for a published work			O	
5.6	Personally written or edited drafts of reports, papers, technical documents, artwork or teaching resources (personal judgement to be exercised)		O	O	O
5.7	Collaborative (multi-agency) technical materials, in draft or final form but not widely disseminated e.g. draft internal project report or deliverable, internal assessments and evaluations,			O	
5.8	Draft and pre-publication forms of resources whose copyright resides with you and/or UCL and from which UCL (or another affiliated party) will derive income or reputation or competitive advantage e.g. draft paper or book manuscript, pre-release software		O		
5.9	Unpublished or licensed final forms of resources whose copyright resides with you and/or UCL and from which UCL (or another affiliated party) will derive income or reputation or competitive advantage (choice of Highly Restricted or Restricted will depend upon the value and uniqueness of the resource) e.g. course-ware, teaching materials, text for use in grant proposals, market analyses, business plans		O	O	
5.10	Student assessments and coursework identified only by a student ID			O	
5.11	Named student work, unless agreed to be widely shared or unless a student contribution to a widely shared work		O		

No.	Description	Secret	Highly Restricted	Restricted	Normal
5.12	Openly shared or public materials, or materials that have not been made public for incidental reasons but could be disclosed without harm to UCL or others				O

3. Security guidance

Having conducted an appraisal of the data held on a particular device or system or server, a decision will need to be taken as to whether the more sensitive classes of information need to be retained in that repository or can be relied upon to be obtained from a better secured repository. For example, Principle Investigators might decide that personal correspondence with or about staff can reside on their UCL workstation and need not be carried on their laptop.

A separate decision will also need to be taken about whether particular classes of data can be stored in a more secure part of a more mixed-sensitivity repository, such as an encrypted disk partition or folder, to be accessed only when explicitly needed.

The guidance notes below are intended only to provide a generic indication of the protection methods that are expected to be applied to the different classes of information. Individual departments, teams and contexts may need to tailor this to handle specific risks or issues relating to the data, devices or environment in which they operate.

Key to sensitivity levels

Secret – very rare – "bunker situation"
Highly Restricted – only for certain named individuals – e.g. recruitment material for a panel
Restricted – maybe to nominated groups, e.g. UCL staff or an inter-university collaboration group
Normal/unrestricted – information that is published for the public or could be disclosed with no risk

Normal/unrestricted – information that is published for the public or could be disclosed with no risk

Printed information

- Data owner should review annually and archive if required.

Electronically stored information

- When disposing of physical media, ensure secure deletion of data. If this is impossible, then destroy the media if it is going to be reused outside of UCL

Restricted – maybe to nominated groups, e.g. UCL staff or an inter-university collaboration group

Printed information

As for normal/unrestricted plus:

- Consider if labelling is required (i.e. inclusion of instructions on the document itself, e.g. "Not for circulation beyond those on this list.").
- Take care to keep to restrict to the intended audience if posting.
- Use a shredder for disposal.
- Store out of sight when not in use.
- Ensure document is accessed only by those who are required to see it (see labelling if used).

Electronically stored information

As for normal/unrestricted plus:

- If data is to be stored on fixed media without access controls and accessible via the web, then it must be encrypted.
- Storage on any system without access controls is not recommended (even when not networked).

- Encryption is recommended for storage on removable media.
- Ensure correct access control for read(including duplication)/write/delete/update access.
- When printing (in particular to shared printing facilities), collect printout ASAP.

Electronically transmitted information

- As for normal/unrestricted plus:
- When faxing, ensure that the recipients are available and consider whether they will be the only person(s) to see the fax.
- If using voice mail, ensure you have reached the correct recipient before leaving a message. You may wish to leave a guarded message in case the voice mailbox is shared – listen to the outgoing message and consider asking for a call back rather than leaving all the information in voice mail.
- It is recommended that secure versions of network applications are used – e.g. ssh, sftp, https and at least WPA for wireless.
- When using email, consider the recipients (take care that reply goes to expected recipients – check any automatically completed fields) and limit circulation whenever possible.

Highly Restricted – only for certain named individuals – e.g. recruitment material for a panel

Printed information

As for restricted, plus:

- Labelling is required.
- Duplication should be limited.
- Consider secure postage to ensure audience is restricted.
- Use a cross-cut shredder for disposal.
- Store in a secure location

Electronically stored information

As for restricted plus:

- If storing on fixed media with access controls, encryption is recommended.
- For storing on fixed media without access controls or for storing on removable media, encryption is required.
- When printing, unattended printing only allowed if printer resides in a locked area. Printouts must be collected ASAP.

Electronically transmitted information

As for restricted plus:

- No faxing allowed.
- Secure versions of network applications must be used – e.g. ssh, sftp, https and at least WPA for wireless.
- Encryption recommended for email.

Secret – very rare – bunker situation

Printed information

As for highly restricted, plus:

- Ensure duplication is very limited.
- Use secure postage to named recipient only.

Electronically stored information

As for highly restricted, plus:

- Encryption required for storage on fixed media with access controls.
- Storage on fixed media without access control not allowed.
- Storage on removable media requires encryption, but is discouraged.
- Disposal of physical media requires physical destruction beyond ability to recover.

Electronically transmitted information

As for highly restricted plus:

- No details to be left on voice mail systems.
- Email not recommended, but encryption required if absolutely necessary to transmit via email.
- File transfer not allowed.
- Local connection to data only.

Appendix A: Risk Assessment

This method of assessing risk considers

- the adverse events that might occur.
- the consequences or impact if the event occurred (to individuals and to organisations).
- how likely the event is considered to be.

In the case of information, the main adverse events may be unintended disclosure (e.g. material accidentally disseminated to the wrong parties or deliberately accessed or intercepted) or the loss of whole repositories (e.g. following loss or theft of a laptop).

Data owners should ensure that risk assessments are undertaken by persons who manage and understand their information and also understand how the devices which could store it are used; e.g. laptops may be regularly left unattended in meeting rooms over lunch or home computers may be used by UCL staff and by their children. This section defines a basic framework for assessing risk, but the judgements about which levels of likelihood and impact apply to you have to be made personally or within your team.

Definitions

Likelihood of threat

Nil	- unlikely to occur	- significantly less than 1 occurrence per year
Low	- may occur occasionally	- of the order of one occurrence per year
Medium	- is as likely as not to occur	- a small number of occurrences (e.g. up to 2 a month)
High	- is very likely to occur	- regular/daily occurrence

Impact on UCL or other organisations or individuals

Nil:	Disclosure is not expected to harm any individual personally or by reputation, will not cause any distress or inconvenience, will not result in any legal liability or disciplinary process, and will have a negligible damage containment cost
Low	Disclosure will result in temporary inconvenience to individual(s) or organisation(s) or minor damage to reputation that can be recovered, and has a small damage containment cost
Medium	Disclosure will cause significant upset to individuals or is expected to result in containment costs and/or financial penalty, or will harm personal or professional or organisational relationships and goodwill.
High	Risk of significant legal liability or severe distress to individual(s) or severe damage to organisational reputation or significant loss of asset value
Unacceptable	Individual(s) placed at risk of physical injury or attack, or risk of large scale (criminal) damage to property or civil infrastructure, or risk of severe and permanent damage to personal or professional or organisational reputation.

Risk assessment score

This table shows how likelihood and impact can be combined to give rise to a risk score. This assessment might be performed for a repository as a whole (for example, for a research database which holds a large quantity of similar kinds of information) or piecemeal to assess the risks of several kinds of information held on a single device. In the latter case, the overall risk score for the

device is equal to the highest scoring kind of information held on it.

	Impact				
Likelihood	Nil	Low	Medium	High	Unacceptable
Nil	1	1	1	1	4
Low	1	2	2	3	4
Medium	1	2	2	4	4
High	1	2	3	4	4

Risk Management

Please use this table to determine the risk classification that applies to the kinds of data you hold on a given device.

Risk factor score	Appropriate management
1	Normal
2	Restricted
3	Highly restricted
4	Secret

The sensitivity classification levels Normal, Restricted, Highly Restricted and Secret relate to sets of protection measures defined in Section 3 of this document. Some examples are given below.

Given that many UCL staff have devices with a complex mixture of information types, Section 2 of this guide provides an inventory of the commoner types of information with a pre-defined mapping to these four sensitivity levels.

Examples

Leaked CV

Likelihood: low/medium
Impact: low/medium depending on whether a CV is part of an active recruitment process or unsolicited
Risk: 2

-> Classification: restricted

Example for leaked details of staff involved in controversial activities

Likelihood: low
Impact: unacceptable (risk of physical attack)
Risk: 4

-> Classification: secret

Example for a very sensitive area of patient identifiable research

Likelihood: Low
Impact: unacceptable
Risk: 4

-> Classification: secret

Appendix B

Handling of printed information (paper, microfiche)

No.	Action	Secret	Highly Restricted	Restricted	Normal/unrestricted
1.1	Labelling of documents (inclusion of instructions on document itself, e.g. "Not for circulation beyond those on this list.")	Required	Required	Consider if labelling is needed	No labelling required
1.2	Duplication of documents	Very limited duplication	Limited duplication	No special handling	No special handling
1.3	Posting of documents	Secure postage[1] to named recipient only	Care to keep to restricted audience – consider secure postage	Care to keep to restricted audience	No particular requirements
1.4	Disposal	Shred – cross-cut	Shred – cross-cut	Shred	No particular requirements
1.5	Storage	Store in secured location	Store in secured location	Clear desk policy – out of sight when not in use	No particular requirements
1.6	Read access	Apply appropriate restriction	Apply appropriate restriction	Apply appropriate restriction	No particular requirements
1.7	Data owner review	Annual review – secure archive if required	Annual review – archive if required	Annual review – archive if required	Annual review – archive if required

[1] A simple way to detect tampering is to sign over an envelope seal and place very sticky tape over this. Consider registered post or recorded delivery for material going out of UCL. Consider checking successful receipt of material.

Electronically stored information

No.	Action	Secret	Highly Restricted	Restricted	Normal/unrestricted
2.1	Storage on fixed media with access controls	Encryption required Special precautions for CC/bank account details	Encryption recommended	No special requirements	No special requirements
2.2	Storage on fixed media without access controls and accessible via the web	Not allowed	Encryption required	Not allowed unless encrypted	No special requirements
2.3	Storage on fixed media without access controls, but not accessible via the web	Not allowed	Encryption required	Not recommended	No special requirements
2.4	Storage on removable media	Consider not allowing this. Encryption required	Encryption required	Encryption recommended	No special requirements
2.5	Read access to information (includes duplication)	Ensure correct access control	Ensure correct access control	Ensure correct access control	Ensure correct access control
2.6	Create/update access to information	Ensure correct access control	Ensure correct access control	Ensure correct access control	Ensure correct access control
2.7	Delete access to information	Ensure correct access control	Ensure correct access control	Ensure correct access control	Ensure correct access control
2.8	Print hard copy	Unattended printing permitted only if physical access controls exist (e.g. locked printer room). Printouts to be collected asap	Unattended printing permitted only if physical access controls exist (e.g. locked printer room). Printouts to be collected asap	Printouts to be collected asap	No special requirements
2.9	Disposal of physical media if the machine is not going to be reused within UCL	Physical destruction beyond ability to recover	Secure deletion of data; if impossible, destruction	Secure deletion of data; if impossible, destruction	Secure deletion of data; if impossible, destruction

2.10	Disposal of physical media if the machine is going to be reused within UCL	Physical destruction beyond ability to recover	Secure deletion of data	Secure deletion of data	Secure deletion of data

Electronically transmitted information

No.	Action	Secret	Highly Restricted	Restricted	Normal/unrestricted
3.1	Fax	Not allowed	Not allowed	Consider recipients	No special restrictions
3.2	Voice mail	No details	Take special care to ensure correct recipient	Take special care to ensure correct recipient	No special restrictions
3.3	Email	Not recommended, but encryption[2] required if absolutely necessary (and compliance with 3.5 below)	Encryption suggested (and compliance with 3.3 above)	Consider recipients and limit circulation (and compliance with 3.3 above)	No special restrictions
3.4	Ftp	Not allowed	Secure ftp	Secure ftp	No special restrictions
3.5	Networks (including Wireless[3])	Consider not allowing. Encrypting applications and/or VPNs required	Encrypting applications and/or VPNs required	Encrypting applications (e.g. ssh, sftp, https) and/or VPNs recommended	No special restrictions
3.6	Other types of connection (e.g. dialup, ISDN, point-to-point link)	Local, encrypted, point-to-point links only	Encrypted links only	Encrypted links only	No special restrictions

[2] Mobile phones are currently out of the scope of these guidelines. Laptop encryption will be dealt with separately and advice is available on the Computer Security Team website on encryption in general.

[3] Wireless users are advised to use encrypted connections (at least WPA)