Information Management Policy

University College London

Document Summary

<table>
<thead>
<tr>
<th>Document ID</th>
<th>TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Approved</td>
</tr>
<tr>
<td>Information Classification</td>
<td>Public</td>
</tr>
<tr>
<td>Document Version</td>
<td>Approved by the Information Risk Governance Group</td>
</tr>
<tr>
<td></td>
<td>12 Sep 2017</td>
</tr>
</tbody>
</table>
1 Policy owner
This policy is owned by the Information Risk Governance Group

2 Policy contact
Head of Information Security

3 History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Approved by</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.12.2015</td>
<td>Draft 11</td>
<td>Bridget Kenyon</td>
<td>Name and role</td>
<td>Initial version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Head of Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.12.2015</td>
<td>Draft 11</td>
<td>SWG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.2016</td>
<td>Draft 13</td>
<td>IRMG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2016</td>
<td></td>
<td></td>
<td></td>
<td>Approved for pilot by IRGG</td>
</tr>
<tr>
<td>12.09.2017</td>
<td></td>
<td>IRGG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 Review plan
This document will be reviewed every two years, or earlier if deemed necessary by the policy owner, e.g. following a change in law.

5 Definitions

5.1 Data versus information
For the purposes of this document, “information” is considered to include both personal data (as defined by the Data Protection Act) and other information, such as intellectual property or financial records.

5.2 Information Owner (IO)
This definition extends the concept of Data Owner (as used in the Data Protection Policy) to include non-personal data.

Each set of information to be classified and managed (e.g. UCL Student Records, or Appraisal records for Finance and Business Affairs Department staff) must have one designated Information Owner.

Owing to the responsibility associated with the role, an Information Owner will typically be a senior staff member of the administration of the local area (e.g. Department), such as Head of Department, or someone nominated by them to take on the role.

5.2.1 Principal responsibilities
- The Information Owner defines which instance of the information is to be considered authoritative (i.e. which is the guaranteed official version).
• The format and location of the authoritative version of the information should be known to the Information Owner at all times.
• The Information Owner is responsible for classifying information—that is, specifying its required confidentiality, integrity and availability.
• They also make decisions on which roles should access information, and what risks are of relevance to the information.
• The Information Owner assigns day-to-day access management responsibilities to the Information Custodian. Ultimately, however, responsibility for the confidentiality, integrity and availability (i.e. the security) of the information remains with the Information Owner.
• The Information Owner liaises with the relevant Risk Management Champion to ensure that the Information Owner is aware of the risks affecting the information. They receive guidance from the Risk Champion on UCL approaches to risk in a given area, and overall decisions on information risk management.

5.3 Information Custodian (IC)
This definition extends the concept of Data Custodian (as used in the Data Protection Policy) to include non-personal data.

The Information Custodian handles the day-to-day management of information (e.g. adding users to access lists). There should be an Information Custodian for every instance of information: so if there are several copies of a CV, sent to several departments, each copy should have a Custodian (if it makes sense, this can be the same person across multiple departments), but there is only one Information Owner, who owns every copy.

The Information Custodian will typically be an administrator or IT manager.

5.3.1 Principal responsibilities

5.3.1.1 Data Management
• Ensure that the information for which they are Custodian is managed in accordance with UCL policies, and the requirements of the Information Owner.
• Act as an escalation point for information management and access issues and breaches.
• Keep abreast of data protection and information security issues.

5.3.1.2 Access & Training
• Ensure that access requests from individuals are thoroughly reviewed, and access is granted only to the appropriate people, and is pertinent to that person’s job role.
• Ensure that access to sensitive information, such as pre-publication research data, financial forecasts, and patient data, is only granted to appropriate roles.

1 Risk Management Champion is as defined in UCL Risk Management Policy and Procedures
within their area, and that individuals in those roles are aware of the sensitivity of such information and the rules for handling it.

- Ensure that changes are dealt with in a timely fashion, such as updating access when a person changes jobs or leaves their area or UCL.
- Regularly review access for their area to ensure it is appropriate.

5.4 Other definitions
Also please see main Glossary:

https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Glossary

6 Introduction
In order for information to be protected effectively, it should be possible to know how important it is to preserve its confidentiality, integrity and availability. It should also be clear what actions are enough to achieve this.

This document explains who is responsible for classifying information, how to classify information, how to label it so that its classification is clear to other people, and how to handle information which has been classified.

Please be aware that the handling information does not list all security measures (controls) which are necessary to protect information, but instead sets a baseline of minimum controls. For example, where risk is higher (e.g. where a large volume of information is stored), controls should be designed to take this into account.

The intent of the document should be borne in mind when interpreting it for a given situation, and it should be interpreted reasonably.

7 Scope
- This policy applies to all information for which UCL is the owner or custodian.
- Where classification/labelling/handling is appropriate, this policy, and no other, shall be used. Classifications described here address not only the required confidentiality of information (which is the usual approach), but also its required integrity and availability.
- The handling scheme in this document applies to all information, whether or not it is labelled.

8 Related documents
8.1 Documents which refer to this policy:
- University College London Records management policy
  https://www.ucl.ac.uk/library/about/records-office/policy

8.2 Documents which this policy refers to:
- UCL Risk Management Policy and Procedures
  http://www.ucl.ac.uk/risk-management/documents/rmpolicy.docx
9 Related requirements

9.1 External requirements
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998

9.2 Internal requirements
- Data Protection Policy:
- UCL Information Security Policy
  https://www.ucl.ac.uk/informationsecurity/policy/policy/public-policy/Policy

10 Stakeholders
The following bodies shall be involved in revisions of this document:
- Information Risk Governance Group
- Information Risk Management Group
- Security Working Group
- Risk Management Working Group

11 Accountable Roles
The policy applies to all staff and students of UCL and all other computer, network or information users authorized by UCL or any department or division thereof. It relates to their use of any UCL-owned facilities (and those leased by or rented or on loan to UCL), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the UCL network; to all UCL owned or licensed data and programs (wherever stored); and to all data and programs provided to UCL by sponsors or external...
agencies (wherever stored). The policy also relates to paper files and records created for the purposes of UCL business.

12 Policy statements

12.1 Information classification scheme
1. The Information Owner (IO) is responsible for classifying information.
2. Classifications shall be reviewed on a suitable timescale determined by the IO. Classifications may change, but confidentiality cannot be regained once lost. In practice, the classification can change.
3. Information shall be classified as follows:

<table>
<thead>
<tr>
<th>How important is this attribute?</th>
<th>Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not important</td>
<td>Public</td>
</tr>
<tr>
<td>Important</td>
<td>Confidential</td>
</tr>
<tr>
<td>Critical</td>
<td>Highly confidential</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How important is this attribute?</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not important</td>
<td>Low Integrity</td>
</tr>
<tr>
<td>Important</td>
<td>Medium Integrity</td>
</tr>
<tr>
<td>Critical</td>
<td>High Integrity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How important is this attribute?</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not important</td>
<td>Low Availability</td>
</tr>
<tr>
<td>Important</td>
<td>Medium Availability</td>
</tr>
<tr>
<td>Critical</td>
<td>High Availability</td>
</tr>
</tbody>
</table>

Confidential and Highly Confidential information shall specify the group(s) which are permitted to view the information.

12.2 Process for classifying data
Use the Information Classification flow chart, which follows, to classify information. Where a local risk rating is different to a UCL-wide rating, then the higher rating shall apply. If a document or repository holds information of mixed classifications, the
highest rating shall apply. Redaction (selective editing to remove information) can be used to reduce the classification of a document where necessary.

Data that is potentially identifiable must be considered carefully. Use the Motivated Intruder Test\(^2\) in these cases.

**Appendix A** provides examples of using the flowchart to classify information.

\(^2\) [https://ico.org.uk/media/1061/anonymisation-code.pdf](https://ico.org.uk/media/1061/anonymisation-code.pdf)
Impact ratings are defined in the UCL Risk Management Policy and Procedures Section 5.2: 
https://www.ucl.ac.uk/risk-management/riskmanagementpolicy
Personal and sensitive personal data are defined in UCL’s Data Protection Guidance: https://www.ucl.ac.uk/finance/legal_services/data_protection/a2z.html

Information Classification Flowchart

Start

Which Attribute?

Confidentiality

Integrity

Availability

Is this personal data?

Yes

Would loss of Integrity result in impacts with rating 4 or 5?

Yes

Would loss of availability result in impacts with rating 4 or 5?

Yes

Highly Confidential

Availability High

Integrity High

Integrity Medium

No

Confidential

No

No

Public

Would loss of Integrity result in impacts with rating 3?

Yes

Would disclosure result in impacts with rating 4 or 5?

Highly Confidential

Yes

No

Would disclosure result in impacts with rating 3?

No

No

Confidential

Public

No

No
12.3 Information labelling
Information labelling is used to indicate the level of protection required for information (e.g. personnel files, emails about disciplinary meetings, printed meeting minutes, research data written in logbooks etc.).

- Information labelling shall be clear and unambiguous.
- Where all material in a given location (e.g. directory, filing cabinet or server) is of the same classification, its location shall be considered sufficient label, as long as the process for extraction of information from the location includes a suitable process for labelling.
- Information with the classification “Public” need not be labelled.
- Information in Word or equivalent format shall be classified by use of a header that appears on all pages.
- Information in other text formats (including paper) shall be classified by a notification at the beginning of the document and on each printed page.
- All labelled documents shall reference the location of this policy where practical.

**WARNING:** Bear in mind that an unmarked piece of information may be “Public” or be of another classification, but as yet unlabelled.

12.4 Information handling scheme
The Information Custodian (IC) shall ensure that handling practices meet the requirements for protection of their information, with reference to this and to other documents as required. Where there is doubt about how to handle the information, this should be referred to the Information Owner or ISG where owner cannot be identified.

Where a third party is involved in handling information, or has the ability to access or alter information, the IC shall ensure that the third party understands and complies with handling requirements.

Classifications are not intended to specify the response to be provided to requests under the Data Protection Act, the Freedom of Information Act, Environmental Information Regulations or the Regulation of Investigatory Powers Act.

In all cases, UCL’s Guiding Principles of information risk management[^3] shall apply.

---

[^3]: See Information Risk Management – Guiding Principles:
https://www.ucl.ac.uk/informationsecurity/policy/internal-policy/information-risk-management-guiding-principles
### 12.4.1 Confidentiality

<table>
<thead>
<tr>
<th>Access</th>
<th>Public</th>
<th>Confidential</th>
<th>Highly confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone may access</td>
<td>Specified groups of roles (e.g. departmental administrators) authorised by IC</td>
<td>Small number of specific roles (e.g. the Principal Investigator for a particular research study and their four staff members) authorised by IC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage</th>
<th>Public</th>
<th>Confidential</th>
<th>Highly confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>No special handling</td>
<td>IT: Adequately encrypted&lt;sup&gt;4&lt;/sup&gt; On systems rated as Level 2&lt;sup&gt;4&lt;/sup&gt; Physical: In secure environment</td>
<td>IT: Adequately encrypted&lt;sup&gt;4&lt;/sup&gt; On mobile devices (e.g. smartphone, laptop, USB stick) only on a temporary basis. Explicit permission from IC required for storage on any personally owned devices On systems rated as Level 3&lt;sup&gt;4&lt;/sup&gt; Physical: Access logged In secure environment (e.g. locked filing cabinet with adequate lock)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Working on</th>
<th>Public</th>
<th>Confidential</th>
<th>Highly confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>No special handling</td>
<td>IT: On systems rated as Level 2&lt;sup&gt;4&lt;/sup&gt; Physical: Only in secure environments</td>
<td>IT: On systems rated as Level 3&lt;sup&gt;5&lt;/sup&gt; Physical: Always attended during use In secure environment Creation of copies (e.g. by photocopying, emailing or printing) to be authorised by IC and recorded</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sending and receiving</th>
<th>Public</th>
<th>Confidential</th>
<th>Highly confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>No special handling</td>
<td>Permission for each type of transmission required from IC Records to be kept of transmission types and recipients by IC Destination facilities to have equal security to source IT: Adequately encrypted&lt;sup&gt;6&lt;/sup&gt; Physical: Secure container</td>
<td>Permission required for each new type of transmission, or new recipient, from IC Destination facilities to have at least equal security to source facilities. Record to be kept of transmission by IC IT: Adequately encrypted&lt;sup&gt;6&lt;/sup&gt; Fax not permitted Physical: Secure container, tracked courier (e.g. delivery by hand), always attended</td>
<td></td>
</tr>
</tbody>
</table>

<sup>4</sup> Storing the password along with the encrypted information is not permitted, as it negates the value of the encryption.
<sup>6</sup> Sending the password via the same means as the information is not permitted, even if in a separate transmission, as it negates the value of encryption.
<table>
<thead>
<tr>
<th>Disposal</th>
<th>IT: Secure deletion using approved tools Physical: Cross-cut shredder or similar</th>
<th>IT: Secure deletion using approved tools with manual verification by IC Physical: Cross-cut shredder or similar</th>
</tr>
</thead>
</table>

### 12.4.2 Integrity

<table>
<thead>
<tr>
<th>Integrity</th>
<th>Integrity Medium</th>
<th>Integrity High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change</td>
<td>Anyone may change</td>
<td>Small number of specific roles (e.g. the Communications Team) authorised by IC</td>
</tr>
<tr>
<td>Specified groups of roles (e.g. web editors for the Physics Department) authorised by IC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>Integrity checking to be applied at intervals defined by IC Version history to be maintained IT: On systems rated as Level 2 Physical: as for confidentiality</td>
<td>One authoritative source of information to be defined by IC Integrity checking to be applied at intervals defined by IC Version history to be maintained IT: On systems rated as Level 3</td>
</tr>
<tr>
<td>Working on</td>
<td>No special handling</td>
<td></td>
</tr>
<tr>
<td>IT: On systems rated as Level 2 Human verification of integrity of processed information as required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sending or receiving</td>
<td>No special handling</td>
<td>IT: Checksums to be used and verified for all transmissions. Physical: inventory of information to be made before delivery and verified after delivery.</td>
</tr>
<tr>
<td>IT: emails to be signed or checksum used. Physical: inventory to be utilised as required.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 12.4.3 Availability

<table>
<thead>
<tr>
<th>Availability</th>
<th>Availability Medium</th>
<th>Availability High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Needs to be available within a week</td>
<td>Needs to be available within a day</td>
</tr>
<tr>
<td>No special handling</td>
<td>Business continuity strategy to be in place. IT: On systems rated as Level 2</td>
<td>Business continuity strategy to be in place and tested for all supporting assets. IT: On systems rated as Level 3</td>
</tr>
</tbody>
</table>

### 13 Sanctions

This policy does not form part of a formal contract of employment with UCL, but it is a condition of employment that employees will abide by the regulations and policies made by UCL. Likewise, the regulations and policies form an integral part of the regulations for students.
Appendix A: Examples of classifying information

The following three examples illustrate how to use the Information Classification Flowchart.

14.1 Bank account details for one individual (for paying in salary)
In this case, we shall assume that the individual is not vulnerable or of national significance. We shall also assume that we are considering a single isolated record, not a record in a database (where multiple records could be lost at the same time, with much higher impact).

14.1.1 Confidentiality
What damage would occur if the bank details were made public?

The flow chart directs us to start by thinking about the Data Protection implications.

This is personal data, but not sensitive personal data. However, from the information in the UCL Data Protection Policy⁷, UCL requires us to treat personal demographic data, such as personal addresses and financial data, with similar care to sensitive personal data. This gives us a confidentiality rating of “Highly Confidential”.

14.1.2 Integrity
What damage would occur if the bank details were wrong?

Loss of integrity, judged on the Local Financial Impact Rating scale on the Risk Management Policy, would produce a financial loss of less than 5% of annual budget to the department. This looks like an impact of 1, giving an integrity rating of Low Integrity. But let’s also check the main Impact Rating Guidelines to be sure.

Here we need to make a number of sensible assumptions to identify the most plausible impact. It is reasonable to suppose that loss of integrity could lead to the individual in question not being paid. It is also reasonable to assume that they would notice, and therefore that this situation would not persist.

Looking at the table of impacts, we can definitely rule out Very High (5) and High (4). We can also argue that Medium (3) is not a plausible impact, as it refers to potential staff, not current staff. This leaves us with Low (2) and Very Low (1). Low (2) seems a better match, as it refers to reputational damage affecting existing staff. It also mentions financial impacts between £250k and £2m; but as long as at least one of the items in the box is a good match, then that is the right classification. This gives us an Integrity Rating of Low (2).

Looking at the flowchart again, this also gives us an integrity rating of “Low Integrity”.

14.1.3 Availability
What damage would occur if the bank details were not there when they were needed?

Loss of availability would have a very similar impact to loss of integrity in this case, so we can reasonably give this information an availability rating of “Low Availability”.

14.2 Medical history for one hundred patients

14.2.1 Confidentiality
What damage would occur if the medical history of these patients were to be made public?

Starting with the question about whether the information is personal data – obviously it is. Is it sensitive personal data? Checking the UCL Data Protection Guidance – it is. So this gives us a confidentiality rating of “Highly Confidential”.

14.2.2 Integrity
What damage would occur if the medical history details were wrong?

This is an interesting question, as it depends on what the information is to be used for. If it is to be used to treat patients, then inaccuracies could be fatal; however, this may not be the case for a given scenario. The Information Owner (IO) should consider the plausible impacts, not apply a generic “all changes will result in death” approach.

Say in this case that the medical data is to be used for nationally important research to determine which treatment for psoriasis will be funded by the NHS. If the wrong information is used, and published, and then the error discovered, then the University would suffer significant reputational damage. The study, in this case, is of national relevance and loss of confidence in UCL may reduce the chances of getting further funding, and possibly affect the next REF evaluation.

If the error is not discovered, then in the worst-case scenario people may be given the wrong treatment for psoriasis, which is going to be unpleasant but probably not fatal. But what if the treatment is more expensive, drawing funding away from other care? This is an indirect impact, which we shall choose to ignore as it is too uncertain to quantify.

Looking at the Local Financial Impact Rating table in the Risk Management Policy, the IO should check how much of the department budget might be affected if there was a loss of confidence in this particular research activity. In
In this case, let’s say it’s 20% of annual budget. This gives us an impact rating of High (4). But let’s also check the main Impact Rating Guidelines.

The main impact rating guidelines table has a variety of different types of impact. The one which is most relevant here is reputational damage; the most likely impact of a loss of integrity of the patient data is (in this case) that funding bodies and collaborators will lose confidence in UCL’s research if it cannot rely upon its research data. This puts the plausible impact at High (4).

Looking back at the flowchart, this gives us an integrity rating of “High Integrity”.

### 14.2.3 Availability

What will be the impact if the patient medical history is not available when it’s needed?

This is really down to the specific circumstances surrounding the information, and should be decided by the IO in consultation with researchers and funding bodies.

In this case, let’s say that the impact of a short-term (under a week) loss of availability is tolerable, and that the information can be re-acquired from the primary source in an acceptable time if required. This gives us an impact (from either of the tables in the Risk Management Policy) of Very Low (1).

Looking at the flowchart, this gives us an availability rating of “Low Availability”.

### 14.3 UCL main web page (www.ucl.ac.uk)

The main UCL web page is not the initial landing page for all visitors; some visitors go directly to a faculty, School, department or research group page from a link in an email or in a non-UCL web page. However, UCL’s front web page does form an important part of the UCL “brand”, and is the first part of UCL that anyone will see if they are researching UCL on the web.

#### 14.3.1 Confidentiality

The page is intended to be freely available to all, hence it has a Confidentiality rating of Public.

#### 14.3.2 Integrity

It is important that the page is not defaced, as reputational damage could occur. The significance of the damage would depend upon the nature of the defacement and the speed of recovery. For this case, we’ll say that recovery could occur within six hours, and that the defacement is malicious but does not contain highly serious content. The impact therefore maps to “Reputational damage (t)/enhancement (o) affecting local community, existing students, potential staff”, and to “Material and/or medium term disruption (t) / enhancement (o) to academic programme delivery/business
14.3.3 **Availability**

There are many different considerations relating to the impact of loss of availability of the UCL website.

- The site is expected to be present continuously (24/7/365); but in practice, occasional outages may be acceptable.
- Repeated outages in a short period may have a more serious impact.
- Response times on the page when navigating to it, and from it to other UCL pages, are important.
- With the changing nature of technology come increased expectations of availability and response time, especially in comparison with competitor sites; so what is a minor issue right now may be much more serious in the future.
- There will be times in the year when outages of the main web page are of far higher importance; e.g. during clearing.
- An incident that removes access to the main web page is very likely to affect other pages as well.

Bearing these considerations in mind, the impact of loss of availability is very hard to quantify. In this case, a good way to proceed is to pick some likely scenarios (e.g. including past incidents), and quantify their impact. This is not infallible, but will suffice.

Say that the University website has been down (for a variety of reasons) five times in the last month. Of these incidents, only one resulted in calls to the ISD Service Desk. The incidents were each resolved within half an hour, and there was no visible reaction on social media or in the news. They occurred during a period when no University-critical events or changes were taking place.

The likelihood of recurrence is not covered here (that is the role of a risk assessment). The impact was low to very low. Had the incidents occurred during a critical period, they would have been of higher, but still not devastating, impact to the University as a whole.

The best guess here is that the impact would have been Low in critical periods, and Very Low during non-critical periods. This would give an Availability rating of Low.

Looking at the “ongoing slow-down” type of incident, where the page remains technically available, but loads very slowly, this is likely to be reported much later, as it is hard to verify and test in many cases, and people tend to tolerate a degree of slow-down before they consider raising an
incident. Tracking down the source of this type of incident is also difficult, and (in the case of a deliberate and malicious attack) finding the cause may not get you to any solution. So for the case of slow-downs which are deliberately induced, the impact is much higher; say Medium. This gives an Availability rating of Medium.

The higher rating takes precedence, so the overall Availability rating is Medium.

15 Approvals

| Endorsed by the Security Working Group | Not Available |
| Endorsed by the Information Risk Management Group | Not Available |
| Approved by the Information Risk Governance Group | 12-Sep-2017 |