Policy

Goldsmiths
UNIVERSITY OF LONDON

Protective Marking

Owner: Senior Information Risk Officer
Review date 20 May 2019

1.0 Purpose

1.1 Protective marking is a labelling system used to indicate the level of sensitivity of documents and information and is used to ensure that information is managed at an appropriate and consistent level of security.

1.2 The more sensitive the information, the higher the protective mark it is given and the more securely it must be managed

1.3 This policy sets out the approach adopted by Goldsmiths, University of London and should be read alongside our Information Security Policy. This sets out the University's overall framework to ensure that information is kept secure and handled correctly and lawfully.

2.0 Policy principles

2.1 **ALL** information that Goldsmiths needs to collect, store, process, generate or share to deliver services and conduct University business has intrinsic value and requires an appropriate degree of protection, whether in transit, at rest or whilst being processed.

2.2 **EVERYONE** who works with the University (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any University information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

2.3 Access to sensitive information must **ONLY** be granted on the basis of a genuine 'need to know' and an appropriate security must be taken.

2.4 Information assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements.

3.0 The protective marking scheme – defining sensitivity levels

3.1 Goldsmiths has aligned its protective marking scheme with the ones used by central and local government and public agencies such as the NHS and Police in order to meet recognised standards (that are based on HMG Security Policy framework) in order to facilitate partnership working.

3.2 Goldsmiths does not handle information at the Top Secret, Secret and Confidential levels. Therefore, the three protective markings or sensitivity levels relevant to University information are:

- Restricted
- Protected, and
- Unmarked / unclassified.

3.0 Protective marking definitions

- **Restricted information**

3.3 'Restricted' is the protective mark used to denote the most sensitive information that is handled in Goldsmiths. The HMG Security Policy Framework defines this as information which, if compromised, is likely to:

- Cause substantial harm or distress to individuals;
- Make it more difficult to maintain the operational effectiveness or security of the UK e.g. emergency response;
- Cause financial loss or loss of earning potential, or facilitate improper gain or advantage for individuals or companies;
- Prejudice investigations or facilitate the commission of crime;
- Breach proper undertakings to maintain the confidence of information provided by third parties;
- Impede the effective development or operation of University policy and decision making process;
- Breach statutory restrictions on disclosure;
- Disadvantage Goldsmiths in commercial or policy negotiations with others;
- Undermine the proper management of Goldsmiths and its services.

3.4 Sensitive personal information as defined by the General Data Protection Regulation is classed as 'Restricted'. This includes information referring to individuals':

- racial or ethnic origin,
- political opinions,
- religious or other beliefs,
- trade union membership,
- health,
- genetics
- biometrics
- sexual orientation,
- sexual life,
- or the commission or alleged commission of offences or criminal proceedings involving them.

3.5 Criminal offence information as defined by the General Data Protection Regulation is classed as 'Restricted'. This includes information referring to individuals' criminal convictions, offences or related security measures.

3.6 This level also includes larger collections of less sensitive person-identifiable information whose loss would could cause only modest distress, but affect many people (hundreds or more).

- **Protected information**

3.7 The 'Protected' mark is for information that is less sensitive than 'Restricted', but still poses risks and needs careful handling. The HMG Security Policy Framework defines this as information which, if compromised, is likely to:

- Cause distress to individuals;
- Breach proper undertakings to maintain the confidence of information provided by third parties;
- Breach statutory restrictions on the disclosure of information;
- Cause financial loss or loss of earning potential, or facilitate improper gain;
- Provide unfair advantage for individuals or companies;
- Prejudice the investigation of or facilitate the commission of crime;

- Disadvantage Goldsmiths in commercial or policy negotiations with others.

3.8 This level includes information relating to living individuals that would enable them to be identified, but which is not so sensitive that it would be classed as 'Restricted'.

- **Unmarked or unclassified information**

3.9 Information that is marked as carrying no classification is often information that is likely to be released into the public domain if requested under the FOI Act or Environmental Information Regulations.

- **Public information**

3.10 In addition to the above markings, the marking 'Public' may also be used where a service wishes to underline that information has been produced for and/or is actively published to the public.

4.0 Applying the protective marking scheme

- **Responsibilities**

4.1 All members of staff must familiarise themselves with the protective marks used by Goldsmiths so that they are able to categorise the information they are handling.

4.2 The author or owner of information is responsible for proactively applying suitable protective marking.

4.3 If a protective mark has not been added to information, the receiver or user of that information should consider whether a protective mark applies and at what level before deciding how to handle the information.

4.4 To manage information appropriately, employees should first identify the appropriate protective mark for information based on its level of sensitivity, then use this as the basis to select suitably secure working practices. The more sensitive the information being handled, the more secure the handling and transit mechanisms that are required for that information.

- **Selecting an appropriate protective mark**

4.5 To determine the correct protective mark, information should be assessed against its fit with the criteria for each level in the hierarchy (see Section 3 above and the table of examples at the end of this document). Making a judgement involves assessing the likely harm and other impacts which could arise if the information asset were to be inappropriately disclosed.

4.6 When applying protective marking, care should be taken to choose an appropriate level:

- Applying too high a protective mark can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of Goldsmiths' business.
- Applying too low a protective mark may lead to compromise of the asset with damaging consequences.

4.7 A mixed set of information should be categorised according to its most sensitive element.

4.8 If there is doubt about the level of sensitivity of a set of information, employees should apply the highest level of sensitivity that they believe is likely until advice has been obtained from Information Governance or an expert within their service on the appropriate level.

- **Marking documents, files and emails**

4.9 Information should be explicitly marked as 'Protected' or 'Restricted' if it is at these levels of sensitivity.

4.10 Emails should be marked [Restricted] or [Protected] in their subject line. All attachments should also be explicitly marked.

4.11 Documents should be visibly marked with their status if they are at the 'Protected' or 'Restricted' level (eg. alongside the title, author and date of issue of a document).

5.0 Usage of the term 'Confidential'

5.1 The term 'confidential' has a specific legal meaning stemming from common case law. For it to provide protection from disclosure, the information must have a number of characteristics that are defined in law. For example, the information has to have been received from a third party (to whom we owe a duty of confidence), it cannot be applied to internally created information.

5.2 The usage of this term should be avoided unless it can be satisfied that the information has the necessary characteristics defined in law. To do so otherwise would provide false comfort that the information is protected from disclosure.

6.0 Committee meetings

6.1 Papers marked as 'Restricted' or 'Protected' should be considered in the closed section of a Committee meeting. These papers should only be circulated to members of the committee who should not forward or share them with others. The unauthorised sharing of papers containing personal data may constitute a breach of the Data Protection Act.

6.2 Papers marked as 'Unmarked / unclassified' or 'Public' may be freely circulated.

7.0 Relationship with the Freedom of Information Act

7.1 Information that is requested under the Freedom of Information Act or Environmental Information Regulations is not automatically protected from release by its protective mark. Each request for information is assessed against the statutory exemptions from disclosure that can be applied and decided accordingly.

8.0 Potential for protective marks to change over the lifespan of information

8.1 It may be necessary to reclassify information:

- Where the potential impact of the information being compromised has changed.
- Where the status of a document has changed (for example where a strategically sensitive report has been finalised for public release).

8.2 Generally speaking, the sensitive of information degrades over time. Wherever possible, protective making should be downgraded as appropriate at the earliest opportunity.

9.0 Related policy documents

Please refer to:

- Information Security Policy.
- Data Protection Policy
- Freedom of Information Act

10.0 Review of policy

This policy will be reviewed prior to the introduction of the General Data Protection Regulations in May 2018 or in the event of a change in relevant legislation or public policy framework.

11.0 Contact list for queries related to this policy

Information Security Manager – Peter Hircock
P.Hircock@gold.ac.uk
020 8228 5963

Data Protection Officer
dp@gold.ac.uk

Senior Information Risk Owner –
Helen Watson
h.watson@gold.ac.uk
020 79197921

Chief Information Officer – Lynne Tucker
Lynne.tucker@gold.ac.uk
020 79197540

Information Governance Manager –
Matthew Ramsey
m.ramsey@gold.ac.uk
020 79197568

Protective mark	Sensitivity and scope	Impact if information was lost or compromised	Examples
Unmarked / Unclassified	• **Non-sensitive information** with limited or no potential to do harm. Does not require special measures to ensure its confidentiality. • **Personal information:** By exception, specific small sets of personal information eg. the salaries of senior officers released under the transparency agenda. • **Other information:** Information published by Goldsmiths, or that could be published in response to a Freedom of Information request.	• Little or no financial impact to Goldsmiths. • No inconvenience or distress to an employee or student • Little or no financial impact to the employee or student • Little or no impact on Goldsmiths' reputation.	• Policies and procedures. • Documents available in the public domain e.g. via Goldsmiths website. • Names and contact details of employees that are in the public domain or where the individual has authorised this. • Training materials.
Protected	• **Moderately sensitive information** whose loss could cause moderate harm. Requires a medium level of security awareness and security practices. • **Personal information:** Information relating to any living individual and which would enable them to be identified. It includes opinions about them and expressions of intention relating to them. • **Other information:** Some business information where there are valid reasons for this not being in the public domain, e.g. it could enable improper gain, lead to loss of earning potential or financial loss.	• Short-term inconvenience, harm or distress to individuals. • Financial loss or loss of earning potential. • Facilitates improper gain. • Breaches statutory restrictions on the disclosure of information (e.g. under the Data Protection Act 1998). • Damage to Goldsmiths' reputation. • Financial impact to Goldsmiths. • Undermines the confidence of information provided by individuals or third parties.	• Personal information relating to any student or employee for which we have a duty of care, e.g. name, address, contact details, National Insurance number, IDs from which the identity of individuals can be looked up. • Documents from employee or student records that **do not contain** "Restricted" type information (see below). • Exempt committee papers excluded from the public. • Draft documents prior to approval for release into the public domain.
Restricted	• **Highly sensitive information** with potential to cause substantial damage or distress to individuals or significant harm in other ways. Needs the most secure management and handling. • **Sensitive personal information**, relating to individuals' racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual life, commission or alleged commission of offences or criminal proceedings involving them. Also, **large sets of personal information** whose loss would affect many people. • **Sensitive business information**, including information defined as confidential **by law**, relating in particular ways to contractual agreements, tenders or commercial operations or which could enable fraud.	• Substantial inconvenience, harm or distress to any number of individuals. • Short-term inconvenience, harm or distress to a large number of individuals. • Causes financial loss or loss of earnings potential. • Facilitates improper gain or advantage. • Substantial damage to Goldsmiths's reputation. Significant financial impact to Goldsmiths (£1m +). • Prejudices the investigation of or facilitates the commission of low-level crime, hinders detection of serious crime.	• Employee or student records which contain information about: **ethnic or racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life, the commission or alleged commission of offences, any proceedings for any offence committed or alleged to be committed.** • **Large amounts of data** at "Protected" level, so that the loss would affect a large set of people (eg. hundreds). • Investigation files.