|  |  |
| --- | --- |
| SOP Title Reference: **Classification of Information** **Policy**  | logomedium |
| Author: **Governance Legal & Assurance Services** |
| **GLAS Policies and Procedures**Classification of Information Policy  |
| St George's, University of London, Cranmer Terrace, London SW17 0RE |

**Contents**

[1. Purpose 3](#_Toc534207114)

[2. Overview 3](#_Toc534207115)

[3. Scope 3](#_Toc534207116)

[4. Policy 3](#_Toc534207117)

[5. Glossary 5](#_Toc534207118)

[6. Authorisation and monitoring 5](#_Toc534207119)

[Document Information 5](#_Toc534207120)

[Document History 5](#_Toc534207121)

# Purpose

St George’s, University of London (St George’s) staff creates and uses information to support its day-to-day business activities and to achieve its research and educational objectives. We all have a role to play in protecting the information we create for use internally and for information we share externally.

This policy outlines the different classifications that can be used to protect our information. Classifying our records supports three key components of information security:

Confidentiality,

Integrity, and

Availability.

# Overview

St George’s information assets [[1]](#footnote-1) must be secured against unauthorised access, disclosure, or modification. Information assets should be classified and accorded different levels of security in relation to their importance and associated duty of confidentiality.

All SGUL information assets should have a classification applied according to:

1. The business value to St George’s
2. Sensitivity of the contents of the information asset,
3. Legal requirements regarding how information is managed i.e., Data Protection Legislation.

# Scope

The policy must be followed by all St George’s employees and contractors who create and handle records as part of their day-to-day activities at the University.

Researchers can access specialised guidance for information they handle at [https://www.St George’s.ac.uk/about/our-professional-services/information-services/library/researchers/research-data-management](https://www.sgul.ac.uk/about/our-professional-services/information-services/library/researchers/research-data-management) the area of the website managed by the Research Data Manager (RDM), or from the RDM themself.

# Policy

1. The classification scheme applies to all information assets regardless of format. Further guidance on the classifications below is available at the end of this document.
	* 1. Public. Information that carries no risk to SGUL if distributed externally. These information assets require no specific security. There is no risk to St George’s if these documents are distributed externally. The classification ‘public’ should be used for information intended to go into the public domain.
		2. Internal. Only accessible to authorised members of staff and if accidentally disclosed could have a negative impact, causing some damage to the reputation of St George’s or distress to the data subjects. This classification will likely cover the majority of St George’s information.
		3. Confidential. Only accessible to relevant members of staff and if disclosed without authorisation will have a negative impact on the employees, reputation, or interests of St George’s. Information assets with this classification have a clear sensitivity due to business or legal value.
2. When choosing a classification be sure not to apply a higher classification than required as this can inhibit distribution; alternatively, if you chose a classification that is too low our information could be at risk.
3. If you have a record set or records series chose the higher classification of the information held within i.e., if you have a record set containing a mix of public and restricted distribution the set will be covered by restricted distribution.
4. It is the responsibility of the Information Asset Owner to ensure that a classification is applied to their records and is visible.

|  |  |  |
| --- | --- | --- |
| **Classification** | **Description**  | **Examples** |
| **Public** | Documents and publications intended for an audience broader than St George’s staff. There is no risk to St George’s if these documents are distributed external to the University. In some cases, contents of the records may need to be redacted i.e., if they are to be released as part of a subject access request or Freedom of Information request. No special security measures need to be applied to these documents. This information is often available via the SGUL website | * Annual Review
* Strategic Plan
* Press Releases
* Strategy 2017 – 2022
* FOI publication schedule and disclosure log
* Published results of research
* Minutes of committee meetings. Minutes should be redacted where appropriate.
 |
| **Internal** | Recipients of disclosed information must respect that it is given to them in confidence.Includes the following categories of personal data: address, age, telephone number | * All HR records.
* Student records
* Contracts
* Procurement information
* Research until publication. Research shared prior to publication will be done so under access conditions.
* Internal phone directory
 |
| **Confidential** | It is likely that only a very small number of documents will be classed as confidential. These documents will likely be related to St George’s strategy or remuneration.Records classified as confidential must have appropriate security controls applied to them to ensure that they are protected against improper disclosure i.e., stored in lockable storage areas, password protected, etc. these records should never be left lying out.Includes the following categories of personal data: race / ethnicity, religion, health, politics, criminal record | * Commercially sensitive records
* Strategy records
* Medical records
* Reserved minutes of committee meetings
 |

# Application of the Policy

Records should be marked with the appropriate classification. For example:



In this example, the ‘Confidential’ classification is added to the subject heading to designate the contents as confidential.



In this example, the ‘Internal’ classification is added at the end of the folders names to designate the contents as for internal use.

Another method to capture the appropriate classification designation is via the use of watermarks.

For records held in databases or on network drives the highest classification designation applied to a record can be applied to all the records held in the database. Records can then be declassified on a case by case basis.

# Authorisation and monitoring

This policy will be reviewed on an annual basis by the Records Manager

|  |
| --- |
| Document Information |
| Document Name | Classification of Information Policy  |
| Author | Kirsten Hylan, Records Manager |
| Next review |  |
| Related policies | 1. [Data Protection Policy](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/data-protection/data-protection-policy)
2. [Information and Technical Security](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/policies-and-procedures/information-technical-security) Policies
3. [Research Data Management](https://www.sgul.ac.uk/about/our-professional-services/information-services/library/researchers/research-data-management)
4. [IG Definitions](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/policies-and-procedures)
 |

|  |
| --- |
| Document History |
| Version | Date | Summary of change |
|  |  |  |
|  |  |  |
|  |  |  |

1. Information Asset -a body of information, defined and managed as a single unit so it can be understood, shared, and protected by SGUL. [IG Definitions Policy](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/policies-and-procedures). [↑](#footnote-ref-1)