BETTER DATA WITH PLYMOUTH UNIVERSITY

Plymouth University

Using the Information Security Classification – Guidance for staff

Author:	Elena Menendez-Alonso (Digital Curator)
Date:	05/01/2016

Security Level:	**PUBLIC**
Status:	Published
Version:	1.0
Reference:	EIM-GDL-001
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/06/EIM-GDL-001-Using-the-Information-Security-Classification-Guidance-for-staff-v1.0.pdf
Review Date:	31/12/2017

1. Introduction

The **Information Security Classification Policy** sets guidelines for classifying and handling Plymouth University information, records and data (whether electronic or hard-copy) based on their level of sensitivity and value to the University.

Key benefits of using the classification include:

- Better understanding of information assets and how they need to be protected.
- Reduced risk of information leaks.
- Identification of information suitable for routine dissemination or for disclosure in the event of a request (e.g., FOI)
- Protection of the rights and interests of the University, its staff and its stakeholders.
- Compliance with legislation such as the Data Protection Act 1998 and the Freedom of Information Act 2000.
- Demonstrable University commitment to good information governance.

2. About this guide

This document provides general guidance on assigning classification levels and interpreting the handling rules provided by the classification.

It is the responsibility of **Information Asset Owners**[1] (or their nominated delegates) to determine the extent to which security classification levels needs to be applied to information in their areas. The security classification of information assets should meet both business and operational needs, being based on an assessment and business impact analysis. Hence, it is appropriate for individual areas to develop local procedures to aid classification of their information assets.

3. Using the Information Security Classification

Step 1: Finding the appropriate classification level

The **Information Security Classification Policy** defines four classification levels:

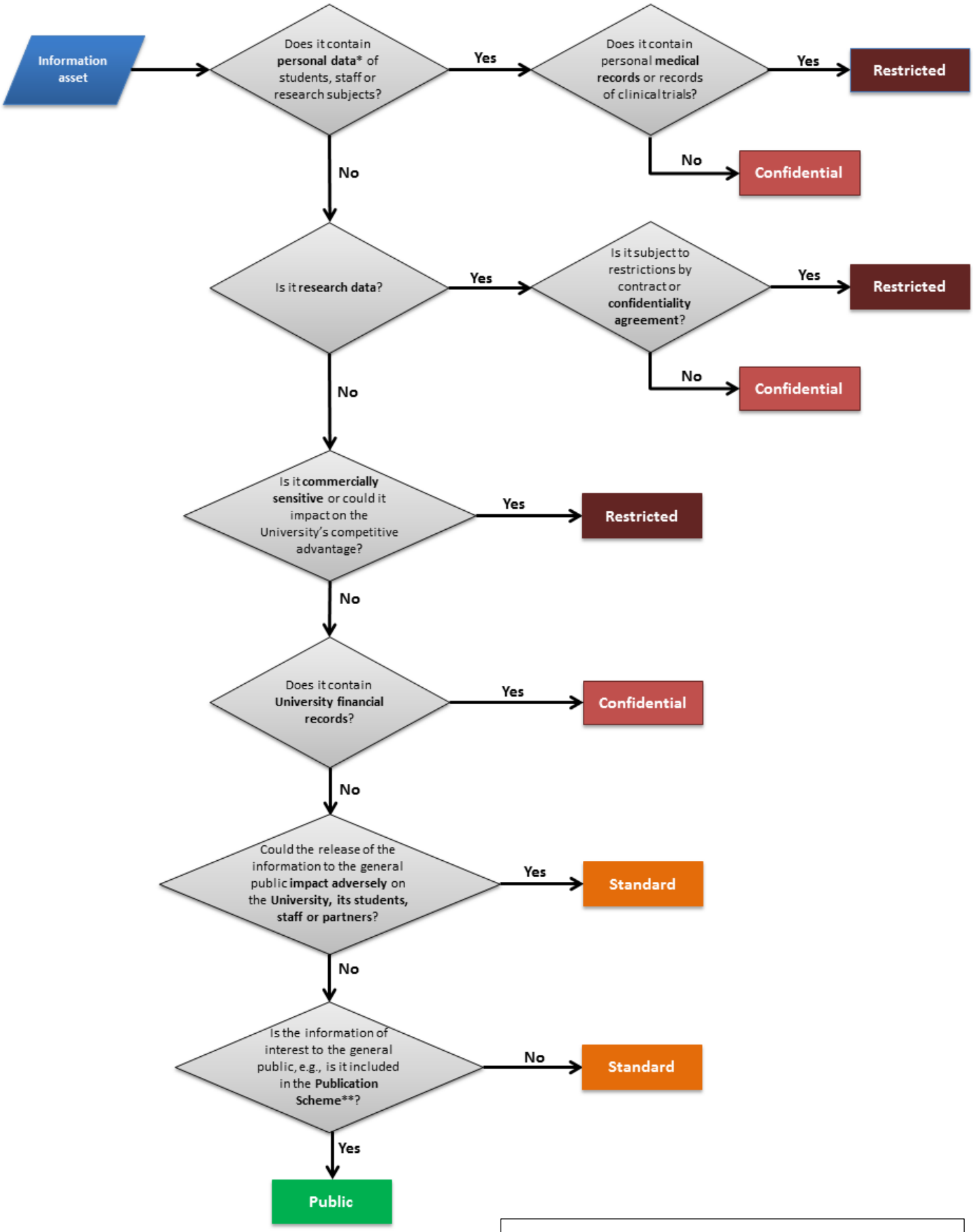
4	**Public**	The information is openly available
3	**Standard**	The disclosure of information would not cause material harm, but the University has chosen not to release
2	**Confidential**	The disclosure of information could cause material harm to individuals or the University
1	**Restricted**	The disclosure of information would cause severe harm to individuals or the University

The recommended security classification should be based on the sensitivity of the information and the impact to the University (e.g.: impact to organisational operations, organisational assets, or individuals) if

[1] Plymouth University. Information Governance Roles & Responsibilities. URL : https://www.plymouth.ac.uk/uploads/production/document/path/2/2980/Information_Governance_Roles_and_Responsibilities_v1.1.pdf. Accessed: 2015-12-11.

the confidentiality, integrity or availability of the information is compromised. You can use the **flowchart** below to perform a **quick risk assessment** on your **information assets**[2].

[2] A valuable or sensitive piece of information, such as an employee or student record, a research dataset, or a financial report.



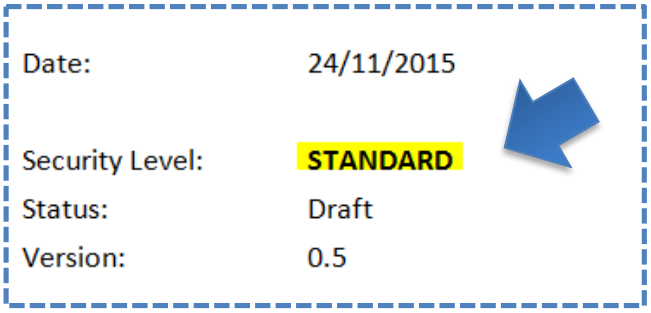
(*) Personal data refers to anything that can provide reasonable deduction about who the data belongs to – i.e. forename and surname or postcode (specifically in remote locations).

(**) For further details see http://www.plymouth.ac.uk/your-university/governance/information-governance/publication-scheme

This flowchart is for guidance. There may be additional factors that determine the classification level of your information. If you have any questions, please contact the IT Service Desk who will route your query to the most appropriate team: https://itselfservice.plymouth.ac.uk.

Step2: Label information and documents with their classification level

Once you have established the classification level of your information, ensure you set appropriate labels, so others know how the information should be handled.



Step 3: Use the handling rules associated with the classification level

Each classification level (public, standard, confidential and restricted) has its own **set of rules** for how that information should be handled. Check the table in the **Information Security Classification Policy** to find the handling rules associated with the relevant classification label.

Classification levels appear across the top of the table, and actions (e.g., viewing or printing) are listed on the first column.

	Public – Level 4	Standard – Level 3	Confidential – Level 2	Restricted – Level 1
Transmission and collaboration	No restrictions.	Document or File encryption suggested. Any distributed documents (electronic or paper) should include **'STANDARD'** in the document header, aligned to the right of the page. Hard printed copy can be transmitted through the normal mail channels.	Document or File encryption required for electronic transmission (for example, via email or secure file transfer protocols). Any distributed documents (electronic or paper) must be watermarked as **'CONFIDENTIAL'** and the intended recipients clearly indicated; if watermarking is not possible **'CONFIDENTIAL'** must be included in the document header, aligned to the right of the page. Printed copies to be delivered in sealed envelopes marked 'Personal' or 'Confidential'.	Document or File encryption required for electronic transmission (for example, via email or secure file transfer protocols). Any distributed documents (electronic or paper) must be watermarked as **'RESTRICTED'** and the intended recipients clearly indicated; if watermarking is not possible **'RESTRICTED'** must be included in the document header, aligned to the right of the page. Printed copies to be delivered in sealed envelopes marked 'Personal' or 'Restricted'.
			For collaboration with external parties a non-disclosure agreement (NDA) is required. A Security Risk Assessment[6] should be performed and approved prior to first use, or after any significant change to the existing service.	

By following the handling rules you will ensure that you know how to proceed before carrying out actions such as storing, editing and emailing information.

4. Related documents and further information

- Information Governance
- Information Governance Roles & Responsibilities
- Data Protection Policy
- EIM-POL-001 Information Security Classification Policy
- Information Security Policies

Document Control			
Version	**Contributors**	**Details**	**Date**
0.1	EMA	Initial draft by E. Menendez-Alonso (Digital Curator)	11/12/2015
0.2	EMA / EW / PF	Review by Emma Wainman (FOI and DP Specialist) and Paul Ferrier (Enterprise Security Architect)	17/12/2015
1.0	EMA	Published version	05/01/2016