GISP11. Information classification

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	All University information will be assigned to an Information Class.
Objective	• To ensure that all information has an assigned Information Class. • To ensure that each Information Class has agreed standards for data storage, handling, transmission and disposal.
Policy	11.1. All information stored on University computer systems will be assigned to an Information Class which will determine how the data is to be stored, handled, transmitted and disposed of. 11.2. Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium. 11.3. Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the organisation and only be removed from site with the permission of the information asset owner. 11.4. All employees to be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Confidential or above. 11.5. Any third party used for external disposal of the organisation's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with this organisation's information security policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non-compliance. 11.6. Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party, must continue to assure the confidentiality and integrity of the information. 11.7. Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

Responsibility	• ITCS will publish and maintain a University approved Information Classification scheme giving guidelines on best practice for storing, handling, transmitting and disposing of data. • Data Managers are responsible for determining a dataset's Information Class using the above scheme, and for ensuring the data is stored and handled in accordance with the guidelines for that Class.
Incident Management	Where data is discovered not to be stored or handled in accordance with its Information Class, this should be reported to the appropriate Data Manager.
Implementation	• The University's information classification scheme and guidance on its application to data is available from https://portal.uea.ac.uk/documents/6207125/6857482/Information+classification+policy.pdf. This policy includes definitions of the following terms: information asset, data owner, data administrator, and data management.