IT Services

University of East London

Data Classification Guidance

1 Introduction

This guidance expands on the principles set out in the University of East London's Data Classification Policy. It gives examples of specific situations and is intended to help you relate your everyday use of IT facilities to the terms set out in the Data Classification Policy. Where a list of examples is given, these are some of the most common instances and the list is not intended to be exhaustive. This guidance forms part of the Information Security Framework and should be read in conjunction with the other policies and guidance contained within the Framework.

2 Purpose

The purpose of this policy is:

- To facilitate understanding of the terms set out in the University of East London (UEL) Data Classification Policy

3 Scope

This guidance can be used by **anyone** using UEL's IT facilities. As well as students and staff it includes, for example:

- Visitors to University of East London web site, and people accessing the institution's online services from off campus;
- External partners, contractor and agents based on site and using UEL's network, or offsite and accessing our systems;
- Tenants of the institution using UEL's computers, servers or network;
- Visitors using the institution's Wi-Fi (Including Cloud);
- Students and staff from other institutions logging on using eduroam.

4 Definitions

Classifying data in an organisation as complex and varied as UEL can seem daunting, however the definitions below have been designed to explain the roles and responsibilities at each level of the business.

Information Asset	An information asset is a collection of any type of data, irrespective of type or format.
Data/System Owner	The Data Owner is the person or Department within UEL who has overall responsibility for the Information asset and for ensuring that it is managed securely and in compliance with University and Government regulations and policies. The Data Owner may delegate day-to-day responsibility for management of the data to a Data Administrator, service group or other persons.
Data Administrator/Data Steward	The Data Administrator/Data Steward is the UEL staff member or department delegated with responsibility for day to day management of the Information asset in accordance with University policies and relevant Government regulations and policies. Processes and procedures used to manage the data should be agreed with the Data Owner. For some data, particularly small datasets, the Data Owner and Data Administrator may be the same person
Security Classification	The Security Classification applied to the Information Asset determines how that Information asset is to be secured.

5 Security Classification

The security classification that a piece of Information receives is based on the level of sensitivity the Information has, and the foreseeable impact on the University should that Information be disclosed, altered, lost or destroyed without authorisation. The classification of Information into different categories ensures that individuals who have a legitimate reason to access a piece of Information can do so, whilst ensuring that it is protected from unauthorised access.

All Information owned, used, created or maintained within the University should be categorised into one of the following four categories:

Public

Information classified as Public relates to the University but can be viewed by anyone. This type of information does not require any specific security measures as it not considered sensitive. Examples of Public Information include:

- University opening times
- Course information
- Marketing material
- Published research
- Staff names, job titles and work contact details
- Faculty names, codes and addresses
- Programme, unit and department names
- HESA subject and fee status codes
- Anything subject to disclosure under the Freedom of Information Act

UEL Internal

Information classified as UEL Internal relates to Information that is available to all authenticated members of UEL staff or enrolled students but is not for public distribution. While the risk to UEL following inappropriate disclosure is low, inappropriate and unauthorised disclosure should be avoided and you should be mindful that when discussing student details, disclosing names and email addresses to third parties outside of UEL without consent may be in violation of the Data Protection Act or other legislation. Examples of UEL Internal Information include:

- Student names and email addresses
- Salary structure and progression information
- Accounting information
- Emails without sensitive data
- Departmental minutes
- Internal communications
- Staff calendar information

Confidential

Information that is categorised as Confidential must be restricted to specific members of staff or students and must not be disclosed without prior authorisation from the person that issued you with the Information. Appropriate security measures must be applied to this category of Information as inappropriate disclosure could cause significant reputational damage and breach contractual and legal obligations. **All documents in this category should be marked 'Confidential'.** This can be done using any appropriate method e.g. written, watermarked, stamped etc. as long as it is clear. Examples of Confidential Information include:

- Staff/ student addresses and personal details
- Next of kin details
- Staff/ student photographs
- Student admission/registration details
- Individual student exam timetables
- Staff/student access cards
- Risk registers
- Budget or finance reports
- Payroll data/HR
- SITS records

Strictly Confidential

Information that is categorised as Strictly Confidential must be restricted to as few staff as is practical and must not be disclosed outside of this group without prior written authorisation from the person that issued you with the Information. Securing this Information should be given significant consideration as inappropriate disclosure would be extremely damaging to the University with extensive negative exposure, financial penalties, and possible legal action. **All documents in this category should be marked 'Strictly Confidential'.** This can be done using any appropriate method e.g. written, watermarked, stamped etc. as long as it is clear. For the avoidance of doubt, sensitive or special category data as defined by the Data Protection Act should be considered strictly confidential.

Examples of Strictly Confidential Information include:

- Staff/student financial data such as bank details
- Staff/student medical history
- Staff/student racial or ethnic origin
- Exam candidate numbers
- Sexual orientation or preferences
- Trade union membership
- Religious beliefs
- Healthcare data
- Disability information
- Biometric data

6 Storage

IT Services offer a range of storage options that meet the security requirements for each Security Classification. Users are encouraged to make use of their allocated OneDrive for Business account, which provides both security and accessibility and enables users to access content from anywhere. If Information is classified as 'Public' users may choose to store Information on other cloud storage platforms such as Dropbox or GoogleDocs, or on personally owned mobile devices. **'Public' information is the only category that is permitted to be stored externally.**

7 Dissemination & Access

Unless Information has been classified as 'Public', users should be mindful of how Information is disseminated paying particular attention to what information is visible to non UEL staff, students and members of the public. Users should follow security best practices to reduce the risk of Information Security breaches. Examples of best practice include:

- Maintaining a clear desk
- Locking workstations when away
- Conducting UEL business on dedicated machines
- Only storing emails in your dedicated Outlook account or on UEL OneDrive for Business

8 Transmission & Collaboration

'Public' information can be freely shared by any means including hard copy. Information designated 'UEL Internal' or above may be transmitted by a number of means depending on sensitivity. For UEL Internal Information, users are permitted to print and email or use sharing funtions on SharePoint, OneDrive for Business, or Yammer. When emailing 'Confidential' or 'Strictly Confidential' Information internally, users are required to ensure that messages are marked as Confidential within Outlook. When transmitting Information outside of UEL, 'Confidential' or 'Strictly Confidential' emails must be encrypted within Outlook.

9 Disposal

Ensuring the appropriate disposal of sensitive Information is a vital step in ensuring security and preventing inappropriate or unauthorised disclosure. For hard copy Information, the most secure disposal method is shredding or, where available, confidential waste containers. When Information that is stored electronically requires disposal, 'Public' and UEL Internal Information can be deleted to the Recycle Bin. Electronic Information designated 'Confidential' or 'Strictly Confidential' should be disposed of securely by contacting the **IT Service Desk.**

10 Responsibilities

Data/System Owners and **Data Administrators/Stewards** are responsible for identifying the appropriate security class for the Information assets within their care and ensuring that the appropriate parameters within the Data Classification policy are applied. Where information is classified as 'Confidential' or 'Strictly Confidential' this must be made clear to those who have access to the data. If management of such data is delegated to other individuals, the Data Owner and Data Administrator must ensure that appropriate guidance is provided.

All projects and services with significant data management and manipulation activities should have a documented data management plan and Information asset register which describes the data to be used, the Security Classification assigned to the data and the identity of the data owners. The plan/register should be made available on request to those authorised by the University to carry out security or data protection audits.

11 Implementation

At the point of creation, all University data must be assigned a security classification and handled in accordance with the Data Classification and Handling Policy.

Other Relevant Policies

a) University of East London: Information Security Policy
b) University of East London: Acceptable Use Policy
c) University of East London: Access Management Policy
d) University of East London: Data Classification Policy
e) University of East London: Access Management Policy
f) University of East London: Cloud Services Policy
g) JANET: Acceptable Use Policy

We appreciate your cooperation in complying with University policy and the Law, and helping keep your device and the University safe and secure. If you are in any doubt, please contact the **IT Service Desk**.

Title	**Data Classification Guidance**
Policy Owner	Andy Cook – Chief Information Officer
Approved By and On	Board of Governors – 24/11/16
Document Type	Guidance
Version	1.0
Review Date	November 2018
Classification	Public