IT Services Policy

Data Classification Policy

1 Introduction

UEL holds many Information assets that must be protected against unauthorised access, disclosure, modification, or other misuse. Efficient management of these assets is also necessary in order to comply with legal obligations including the Data Protection Act, General Data Protection Regulation and the Freedom of Information Act.

2 Purpose

The Purpose of this policy is:

- Provide a framework for classifying and handling data to ensure that the appropriate degree of protection is applied to all data held by the University.
- Use appropriate classification to determine how the data should be accessed and handled
- To ensure that sensitive and confidential data remains secure.

3 Scope

This policy forms part of the Data Protection Framework and is to be applied to all Information held by the University, including data and documents relating to UEL teaching, students, research activities and administration. The policy applies to information held in all formats including electronic and paper based Information.

4 Implementation

At the point of creation, all University data will be classified and handled in accordance with a Security Classification. The categories of classification are:

- Public - Information that relates to the University but can be viewed by anyone inside or outside of UEL e.g. Opening times etc.
- UEL Internal - Information that is restricted to members of UEL staff or students and not for widespread public distribution e.g. internal emails etc.
- Confidential – Information that is restricted to specific members of UEL staff or students that must not be disclosed without prior authorisation. **All documents in this category should be marked**

'Confidential' e.g. Staff/Student personal details etc.

- Strictly Confidential – Information that relates directly to sensitive or high risk data. **All documents in this category should be marked 'Strictly Confidential'** e.g**.** a students disability status, business critical negotiations etc.

By default, and in keeping with the core function of a University all data are classed Public (accessible to the world). If one of the other security classifications is applied to data, this data must be protected as set out below. Further detailed guidance can be found in the Data Classification Guidance document.

5 Security Classifications

Public	e.g. Opening times, prospectuses, open day schedule, published research, vacancy details etc.
Acceptable Storage Methods	• Public-facing web pages • Centrally managed home drive • OneDrive for Business • External, personally owned devices
Acceptable Dissemination & Access Methods	• Widely available • Unrestricted dissemination via electronic or hard copy • Dissemination must not violate any applicable laws or regulations. • Information should be identifiable as from UEL • Permissions to modify limited to authorised users
Acceptable Transmission & Collaboration Methods	• Internet • Internal and personal email • Third party storage • Printed Copy
Risk	None – this is general information with no particular sensitivity
Example Security Measures	None necessary
Acceptable Disposal Methods	No restrictions but recycle where possible

UEL Internal	e.g. Accounting information, student communications, process outputs, internal emails, minutes, communications
Acceptable Storage Methods	• Centrally managed home drive • OneDrive for Business • Personally owned devices signed up to Mobile Device Management
Acceptable Dissemination & Access Methods	• Available across the University • Available to University staff electronically by authentication • Internal emails should not be forwarded to personal email accounts (Gmail, Hotmail etc.) • Hard copy information should be kept out of public areas • Information should be identifiable as from UEL • Permissions to modify limited to authorised users

Acceptable Transmission & Collaboration Methods	• Internal email • Shared Folders • SharePoint • Staff Intranet • OneDrive for Business sharing with Staff and authorised 3rd parties
Risk	Low – however inappropriate to disclose to third parties in most cases. Accidental disclosure should be managed (see guidance).
Example Security Measures	• Send by UEL email only • Store using IT approved methods • Hard copy Information should be stored within business areas • Where content is uploaded to the UEL intranet, ensure the correct sharing permissions are associated with the content
Acceptable Disposal Methods	Electronic copies – normal deletion methods Hard copies – Shredding or secure disposal

Confidential: **All documents should be marked 'Confidential'**	e.g. Documents containing personal data, employee/student records, sensitive business data, financial data, sensitive research etc.
Acceptable Storage Methods	• Centrally managed home drive • OneDrive for Business
Acceptable Dissemination & Access Methods	• Available only to those that need to know for their role or function • Only available for specific purposes • Confidential emails **must not** be forwarded to personal email accounts (e.g. Gmail, Hotmail etc.) • All email should be marked 'Confidential' • Hard copy Information should be stored in secure areas • Printed copies to be delivered by hand directly to the recipient
Acceptable Transmission & Collaboration Methods	• Internal email following 'Need to Know' principle and the message marked as Confidential in settings. • If sending to an external third party, email must be encrypted • Limited OneDrive for Business sharing with required staff and authorised third parties only • Any distributed documents (electronic or paper) to be marked as 'Confidential' and the intended recipients clearly indicated • Appropriate third party storage can be used provided encryption /appropriate security controls are in place
Risk	High – Inappropriate disclosure could cause significant reputational damage and breach contractual and legal obligations
Example Security Measures	• Store on centrally managed filestore with secure access controls applied • Store on OneDrive for Business • Where information is stored on portable electronic storage devices or media, that storage must be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only authorised individuals having access
Acceptable Disposal Methods	For electronic deletion contact IT Services For hard copies – shredding or confidential waste disposal container

Strictly Confidential (All documents should be marked 'Strictly Confidential')	e.g. special category data such as medical or ethnicity data, business critical information, PREVENT case documentation, University banking information etc.
Acceptable Storage Methods	• Centrally managed home drive • OneDrive for Business
Acceptable Dissemination & Access Methods	• Available only to those that need to know • Only available to specific University staff • Emails containing strictly confidential data must not be forwarded externally • All email should be marked 'Confidential' with contents and attachments encrypted • Hard copy Information should be stored in secure areas with access logged. Removal off site should be minimised • Printed copies to be delivered by hand directly to the recipient • Electronic access to the Information should be recorded
Acceptable Transmission & Collaboration Methods	• Internal email following 'Need to Know' principle and the message marked as Confidential in settings. • External third party email must be encrypted • Limited OneDrive for Business sharing with required Staff and authorised third parties. Access and sharing should be recorded • Any distributed documents (electronic or paper) to be marked as 'Confidential' and the intended recipients clearly indicated • Appropriate 3rd party storage can be used provided encryption /appropriate security controls are in place
Risk	Very High – inappropriate disclosure would be extremely damaging to the University with extensive negative exposure
Example Security Measures	• Store on centrally managed filestore with secure access controls applied • Store on OneDrive for Business or Sharepoint with advanced permissions • Where information is stored on portable electronic storage devices or media, that storage must be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only
Acceptable Disposal Methods	For electronic deletion contact IT Services For hard copies – Shredding or confidential waste disposal container

6 Responsibility

Data Owners, Data Administrators and **Business Owners** are responsible for identifying the appropriate security classification for Information assets within their remit and ensuring that the appropriate data management policies governing storage, dissemination, disposal etc. are followed. Where information is classified not for public consumption (i.e. UEL Internal, Confidential or Strictly Confidential) this should be made clear to those who have access to the data. If management of such data is delegated to other individuals, the System owner must ensure that appropriate guidance is provided.

7 Other Relevant Policies

a) University of East London: Information Security Policy
b) University of East London: Data Protection Policy
c) University of East London: Acceptable Use Policy
d) University of East London: Data Retention Policy
e) JANET: Acceptable Use Policy

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