# The Data Retention and Erasure Policy Summary

This document will give a short summary of the contents of the Data Retention and Erasure Policy . It applies to personal data only and applies to all staff within University of Plymouth.

## Retention Procedures and Guidelines Records

Records are kept - to effectively and compliantly carry out our everyday business functions. Records will be created, maintained and retained to provide information about, and evidence of the University of Plymouth's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** document available on our website.

## Retention Periods

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All University of Plymouth and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines as stated in the policy.

## Designated Owners

Owners are assigned based on role, University area and level of access to the data required. All systems and records have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Has knowledge and will authorise any review, removal, destruction or access to data and records.

Owners of data classifications will be responsible for setting the retentions schedule for that item and reviewing/updating it on a yearly basis.

## Document Classifications

The classification is used to decide what access restriction needs to be applied and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

We utilise 5 main classification types

- **Unclassified** - information not of value and/or retained for a limited period where classification is not required or necessary
- **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
- **Internal** - information that is solely for internal use and does not process external information or permit external access
- **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
- **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

For a full list of classifications please read the Information Security Classification Policy: here.

## Suspension of erasure

If University of Plymouth is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against University of Plymouth, then the need to erase data in line with the retentions schedule will be suspended until the audit/investigation is completed.

Document Archival

Documents are grouped together by category and then in clear date order when stored or archived, once the retention period has elapsed they will be reviewed or confidentially destroyed.

Expiration of Retention period

Once data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

Destruction and disposal of Records

- All Paper and electronic records are disposed of in an ethical and compliant manner
- Data Sticks are disposed of by incineration
- Destruction/disposal of ssystems, computers and technology equipment must be organised by TIS

Erasure

Data subjects only have a right to have personal data erased and prevent processing if as per the *below conditions:*

Data Subject Request (SAR)

- Data is no longer necessary in relation to the purpose for which it was originally collected/processed
- In order to comply with a legal obligation
- Data was unlawfully processed
- The individual objects to the processing and there is no overriding legitimate interest for continuing the processing

This is carried out by the Data Protection Officer in conjunction with any department manager and the IT team to ensure that all data relating to that individual has been erased.

Responsibilities

Deans, Heads of Directorates and information asset owners have overall responsibility for the management of records and data generated by their departments and are managed in a way which meets the aim of the policy. DPO must be involved in any data retention and records processes including archiving and destruction. Employees records they are responsible for are complete and accurate and that they are disposed of in accordance with the University of Plymouth's protocols.

ERDF

ERDF grant recipients are required to provide records to evidence that the expenditure in claims complies with the relevant regulations, rules and terms of the Funding Agreement. All projects are required to retain documents for a period after the activity has ended.

Retention Records

University of Plymouth regulatory, statutory and business retention periods and the subsequent actions upon reaching those dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year.

If you require further clarification or information please read the full policy which can be found on our website.