UNIVERSITY OF PLYMOUTH

Data Retention and Erasure Policy

Author:	Mike Godfrey
Date:	08/10/2018

Document Security Level:	PUBLIC
Document Version:	1.0
Review Date:	Q4 2019

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Mike Godfrey	GDPR Consultant	Initial Draft	12/06/2018			
0.2	Mike Godfrey	GDPR Consultant	Comments added after 1st Review	06/07/2018			
0.3	Mike Godfrey	GDPR Consultant	Final draft	22/08/2018			
1.0	Mike Godfrey	GDPR Consultant	Published version	01/10/2018	Information Governance Committee		13/09/2018

1. Contents

1 Introduction

In May of 2017 the GDPR laws came into effect and they fundamentally changed the way we treat personal data and the owners of the data. This policy is in place to ensure all staff (including temporary and contractors), visitors and students are aware of their responsibilities and outlines how the University of Plymouth complies with the core principles of GDPR in relation to the University's approach to data retention and erasure.

The University of Plymouth recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of University of Plymouth. This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records, and data management is necessary to:

- Ensure that the University conducts itself in a structured, efficient and accountable manner
- Ensure that the University realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core University functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The University of Plymouth only ever retains records and information for legitimate or legal business reasons and always complies fully with the data protection laws, guidance and best practice.

2 Purpose

The purpose of this document is to provide University of Plymouth's statement of intent on how it provides a structured and compliant data and records management system. We define ***'records'*** as all documents, regardless of the format; which facilitate the Universities activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

.

3 Scope

This policy applies to all staff within the University of Plymouth *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the University in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 Personal Information and Data Protection

The University of Plymouth needs to collect personal information about the people we employ, work with or have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include *(but is not limited to),* name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. We are committed to collecting, processing, storing and destroying all information in accordance with the *General Data Protection Regulation*, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle:

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation').**

5 Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the University of Plymouth's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to the University of Plymouth and are an important operational asset. A systematic approach to the management of our records is essential to

protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

The University of Plymouth's objectives and principles in relation to Data Retention are to:

- Ensure that the University of Plymouth conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant retention, erasure and destruction
- To develop and maintain an effective and adequate records management program to ensure effective archiving, review and destruction of information
- To only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed

6 Guidelines & Procedures

University of Plymouth manage records efficiently and systematically, in a manner consistent with the GDPR requirements, and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

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 will be found in the published ***Record Retention Schedule*** found on the University's website.

It is our intention to ensure that all records and the information contained therein is:

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Monitored** – staff, University of Plymouth and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

6.1 Retention Period Protocols

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.

For all data and records obtained, used and stored within the University of Plymouth, we:

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas: -
    - the requirements of the University of Plymouth
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects
- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, University of Plymouth will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- Transfer paper based records and data to an alternative media format in instances of long retention periods (*with the lifespan of the media and the ability to migrate data where necessary always being considered*)

6.2 Designated Owners

All systems and records have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, University area and level of access to the data required. Data and records are never reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owners. These owners will also be responsible for continually reviewing the retentions schedule for items that they own, ensuring accuracy by updating the schedule accordingly if any retention periods or details have changed.

6.3 Document Classification

The University of Plymouth have a detailed Information Asset Register (IAR) for identifying, classifying, managing, recording and coordinating University of Plymouth's assets (*including information*) to ensure their security and the continued protection of any confidential data they store or give access to. The University of Plymouth utilise the Information Asset Register (IAR) to document and categorise the assets under our remit and carry out regular Information Audits to identify, review and document all flows of data within University of Plymouth.

The University of Plymouth also carry out regular Information Audits which enable us to identify, categorise and record all personal information obtained, processed and shared by our University of Plymouth in our capacity as a controller and processor and has been recorded in the IAR and includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Retention periods
- Access level (*i.e. full, partial, restricted, etc.*)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types. See the Security Classification Policy on the university's website

We utilise 5 main classification types:

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

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.

6.4 Suspension of Record Disposal for Litigation or Claims

If the 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 the University of Plymouth, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

6.5 Storage & Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed depending on their purpose, classification and action type.

7 Expiration of Retention Period

Once a record or 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.

7.1 Destruction and Disposal Of Records and Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The University of Plymouth is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

7.1.1 Paper Records

Due to the nature of our business, the University of Plymouth retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The University utilises onsite-shredding or a professional shredding service provider to dispose of all paper materials.

Employee shredding machines and confidential waste sacks are made available in most buildings and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

7.1.2 Electronic & IT Records and Systems

The University of Plymouth uses numerous systems, computers and technology equipment in the running of its business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active; this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date register of destroyed records.

Only the IT Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Department is responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Department to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

7.1.3 Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support *(i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 2 years.

Examples of correspondence and routine memoranda include (but are not limited to): -

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

When a data stick is found and handed to security for safe keeping it will remain there for 28 days. If after that period the data stick is not claimed it will disposed of.

8 Erasure

In specific circumstances, data subjects' have the right to request that their personal data is erased. However the University of Plymouth recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies:*

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and the University of Plymouth received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out under instruction 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.

These measures enable us to comply with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed:

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where University of Plymouth has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. ***Such refusals to erase data include:***

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

8.1 Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Act 2018, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.
Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

9 Compliance and Monitoring

The University of Plymouth is committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

10 Responsibilities

Heads of Faculty, Heads of Departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy. Where a DPO has been designated, they must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with University of Plymouth's protocols.

11 ERDF Requirements

The ERDF Funding Agreement states that 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, to enable the Managing Authority to meet is reporting obligations and to demonstrate compliance with EU requirements.

Good record keeping is an essential project management tool. By keeping orderly and comprehensive records, grant recipients will find it far easier to assess and report on the project status and progress in monitoring the project.

Record retention is an important consideration in the development and delivery of a project funded by ERDF. Projects can be subject to an audit even after the project is completed and it is therefore a requirement of grant that core documents are retained and made available for inspection over the entire period. Failure to produce adequate and satisfactory evidence can result in the repayment of grant.

To ensure that this process is followed, all applicants are required to produce and provide as evidence, policies for specific areas including document retention. This reference can be included in current policies that the grant recipient already uses or separate policies specifically developed for the ERDF project to follow.

For projects delivered by a consortium of partners, it is the Grant Recipient organisation that is responsible for the audit trail. The Grant Recipient must make sure that any delivery partners or sub contractors keep adequate records. To do this, they will need to show that they have systems in place to verify the information provided and held by partners.

11.1 How long records should be kept for?

All projects are required to retain documents for a period after the activity has ended and these should be kept in an acceptable format so that they can be inspected where necessary. The grant recipient will be informed of this retention period at the end of the project. The period is dependent on the date at which the final claim is submitted to the Managing Authority so the retention period will be unique to each project and this period cannot be specified at the outset.

As a minimum, all documents must be retained for two years after the Audit Authority submits the Annual Control Report in which the final expenditure for the completed project is included. This should not be interpreted by grant recipients as two years after the project submits its final claim. This is to ensure documents may be made available to the European Commission and European Court of Auditors upon request in accordance with Article 140(1) of Regulation (EU) No 1303/2013.

There are other document retention requirements in addition to this rule:

- Grant Recipients must comply with and assist the Managing Authority to comply with document retention requirements under any applicable State Aid rules. Where Projects are operating under a State Aid scheme in accordance with the General Block Exemption Regulation (Commission Regulation (EU) No 651/2014) or De Minimis Regulation (Commission Regulation (EU) No 1407/2013), Grant Recipients must maintain detailed records with the information and supporting documentation necessary to establish that all the conditions laid down in the Regulation are fulfilled. Such records must be kept for 10 years after the last aid is granted under the scheme. For ERDF Projects, the last aid may not be granted under a scheme until 2023 meaning that documents will need to be retained until 2033.
- Grant Recipients will also need to retain documents to evidence compliance with the EU Regulations governing ERDF Funding. In particular, revenue generating projects covered by Article 61 of Regulation (EU) No 1303/2013 may have to retain documents for a longer period, which will vary depending on the nature of the project, to enable the revenue to be calculated. See the Guidance on Revenue Generating Projects on the DCLG website.
- Where applicable, Grant Recipients will also need to retain documents to demonstrate compliance with Article 71(1) of Regulation (EU) No 1303/2013. This sets out the conditions applying to any project which involves investment in infrastructure or 'productive investment' and under its terms all (or a proportion of) the funding must be paid back if (subject to exceptions):

    - within 5 years, or for Projects concerning the maintenance of capital ("infrastructure) or jobs created by small and medium sized enterprises, within 3 years (or the relevant period set out in State Aid rules, where applicable) any of the following applies:
    - the production stops or is relocated outside the programme area;
    - ownership of the infrastructure (building/capital investment) is changed, giving a firm/public body an undue advantage;
    - there is a substantial change in the project affecting its nature, objectives or implementation conditions which has the effect of undermining its original objectives.
    - In addition, Article 71(2) sets out the circumstances in which funding is to be paid back where productive activity is relocated outside the EU.
    - Grant recipients will also need to be able to provide evidence that they have complied with their obligations under the ERDF Funding Agreement. In particular, where funding is provided for fixed assets such as land, buildings, plants and machinery or other assets treated as major assets in the Funding Agreement, grant recipients will need to be able to provide evidence that these assets have continued to be used for their approved use and have been retained for an agreed period i.e. for no aid projects this is five years from the final payment to the beneficiary or 3 years in cases concerning the maintenance of investments or jobs created by SMEs. Where the ERDF contribution takes the form of State Aid, the period shall be replaced

by the deadline applicable under the State Aid rules. Accountancy rules, or rules relating to sources of match funding may also have longer periods, so the documentation retention policy for the project will need to take account of these points.

Prior to the destruction of any documents, confirmation should be sought from the Managing Authority.