**DATA RETENTION POLICY**

**EFFECTIVE: DD/MM/YYYY**

**Important:** This is a generic template document. It requires

tailoring specifically for your organisation before being published. Professional advice should be taken before applying it.

**Should you require any further assistance then please contact the DPO Centre at** [www.dpocentre.com](http://www.dpocentre.com)**.**

Copyright©: The DPO Centre

# CONTENTS

[CONTENTS 2](#_Toc42074906)

[1 INTRODUCTION 3](#_Toc42074907)

[2 SCOPE 3](#_Toc42074908)

[3 RETENTION PROCEDURE 4](#_Toc42074909)

[4 RETENTION OF ENCRYPTED DATA 4](#_Toc42074910)

[5 RETENTION OF DIGITAL DATA 5](#_Toc42074911)

[6 ARCHIVING AND RETENTION OF DOCUMENTATION 5](#_Toc42074912)

[7 ARCHIVING PROCESS 5](#_Toc42074913)

[8 DISPOSAL OF RECORDS 6](#_Toc42074914)

[9 DISPOSAL OF ELECTRICAL HARDWARE 6](#_Toc42074915)

[10 DOCUMENT OWNER 7](#_Toc42074916)

# INTRODUCTION

This Retention Policy (“Policy”) applies to [ORGANISATION].

For the purpose of this Policy, the terms ‘document’ and ‘records’ include information in both hard copy and electronic form and have the same meaning hereby referred to as Documents or Documentation.

In certain circumstances it will be necessary to retain specific records in order to fulfil statutory or regulatory requirements and to meet operational needs. Any retention of specific records should be retained under the retention period specified in our Retention Schedule which can be found here: [link or indicate location].

Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation)  (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003, all of the foregoing as amended from time to time, and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

# SCOPE

[ ORGANISATION ] is bound by various obligations with regard to the documentation and electronic data it retains. These obligations include the period of retention for Documentation and when and how this documentation is disposed.

Data Protection Legislation provides “personal data must 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”. The purpose of this Policy is to ensure that necessary records, documents and electronic data of ORGANISATION are adequately protected, archived and disposed of at the correct retention period, and to provide all staff with clear instructions regarding the appropriate retention and disposal of documentation.

This Policy will also help ameliorate paper records and electronic data storage issues identified throughout the business and to eliminate the need to retain paper and electronic records unnecessarily.

ORGANISATION will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it is required to hold to meet its statutory functions and the provision of its services.

This policy covers all personal data that the ORGANISATION holds or has control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings.

This policy covers data that is held by third parties on behalf of ORGANISATION, for example cloud storage providers or offsite records storage. [Delete if not relevant – It also covers data that belongs to the ORGANISATION but is held by employees on personal devices in accordance with our Staff Bring Your Own Device Policy.]

# RETENTION PROCEDURE

All decisions relating to the retention and disposal of documents should be taken in accordance with this Policy and the Retention Schedule.

In circumstances where a retention period of a specific document has expired, a review should always be carried out prior to a decision being made to dispose of the record.

# RETENTION OF ENCRYPTED DATA

Any information retained under this Policy that is in an encrypted format, consideration must be taken for the secure storage of any encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

# RETENTION OF DIGITAL DATA

Any digital data including media and email files are retained [specify where and how]. The backup of electronic data is [specify how and where and time limits].

The process for accessing stored electronic data is [specify how] [state how access is authorised and mechanically affected and how records are protected from loss, destruction or falsification during this process].

All portable / removeable storage media are destroyed [specify how and when]

All cryptographic keys, which are required for [identify record types] are retained [specify where and how].

# ARCHIVING AND RETENTION OF DOCUMENTATION

Archiving is defined as the process by which inactive data, in any format, is securely stored for long periods of time in accordance with a Retention Schedule.

[ORGANISATION] archives paper records [state offsite or onsite] [If offsite state name of company].

All documentation should be retained for twelve (12) months on site in a secure location, at the end of the twelve (12) month period all documentation will be collected by [Add company] [Amend to be company specific]

There may be exceptions where documentation will need to be retained for longer periods at site, in these instances the [Add role] will be responsible for ensuring that the documentation is held in a safe and secure location.

# ARCHIVING PROCESS

The method of archiving selected for a particular document will vary between departments and services. Any questions regarding archiving should be raised in the first instance with the department manager.

In all cases identify the documents that need to be retained in accordance with the Retention Schedule. Prior to archiving, all duplicates and any unnecessary papers should be removed. Standard Archiving Boxes should be obtained, clearly labelled and correctly sealed.

[Add in company archiving details if 3rd party used]

# DISPOSAL OF RECORDS

Any record containing confidential information must be [disposed of in a confidential waste bin or - delete if not used] shredded using a cross-cut shredder.

Disposal of documents that do not contain confidential information may be disposed of in the normal way or recycled.

Records of disposal should be maintained by each department and should detail as a minimum the document disposed of, the date of disposal and the person who authorised the disposal.

# DISPOSAL OF ELECTRICAL HARDWARE

IT equipment and devices that have the ability and capability to store personal data include:

* PC’s
* Laptops
* Mobile Phones
* Multi-Functional Devices – printers / scanners
* Servers
* USB Memory Sticks and external hard drives.

IT equipment disposal must be managed by [Add role] [specify if under separate policy]

All computer equipment, recycling or refurbishing must be disposed of in accordance with the Waste Electric and Electronic Equipment Regulations 2013. [Please also refer to our separate IT Disposal Policy.]

# DOCUMENT OWNER

[Add name or role] is the owner of this document and is responsible for ensuring that this Policy is reviewed in line with the review requirements of Data Protection Legislation.