CAMBRIDGESHIRE
& PETERBOROUGH
COMBINED AUTHORITY

# Retention Policy

| | |
|---|---|
| Type of document: | Guidance |
| Document produced by: | Cambridgeshire & Peterborough Data Protection Officer |
| Document approved by: | Cambridgeshire & Peterborough Combined Authority Board |
| Version : | Version 2 |
| Issue date: | |
| How is this shared? | Electronically |
| Date due for review: | Annually April |
| Reviewer: | Susan Hall |

| **Data Protection Contact** | | |
|---|---|---|
| **Contact Details** | **Email** | **Phone** |
| Susan Hall | dpo@cambridgeshirepeterborough-ca.gov.uk | 07706 341719 |

# Contents

# Introduction

Information can be one of our most important resources we have. We have to manage it and that means making sure we keep information for the right length of time and destroy it securely when we don't need it anymore. The implementation of good records management and records retention practices will benefit the authority in many ways.

It's not just about Data Protection Act 2018 ("DPA") or the UK General Data Protection Regulations ("UK GDPR"). The Freedom of Information Act 2000 plays a part as well and places a legal obligation on us to make available information we hold.

However, neither the Data Protection Act / UK GDPR nor the Freedom of Information Act tell you how long to keep something for. There is usually another piece of law that tells us that like HMRC rules or acts relating to children for example.

This policy applies to all records held whether they are paper copy, CD, on the network, cloud or computer systems.

# "If you only read this…"

Do know how long you should keep a record

Do keep a record of what has been kept and where

Do make sure you destroy securely

Do make sure you destroy when you should

Do keep a record of what you destroy and when

Do ask the Data Protection Officer for advice and help

Don't keep personal information just because it could be useful

Don't ignore retention schedules, it is all part of good records management

# Quick questions

### How do I know how long to keep a record?

There is no hard and fast one timescale fits all approach. It will depend on the type of record and what legislation like HMRC rules says. Check the schedule for what the document is about and then we can determine how long we should keep it for.

### What do I do if I am not sure?

Ask. It is better to double check and help make sure our retention schedule guidance is up to date.

### Should I use email as a place to keep records?

No. You should not keep personal information about customers or staff you manage in your email. It should be saved to a line of business system or a network folder. If you leave, the authority still has a need to gain access to that information.

### How do I destroy securely?

We have a shredding cupboard and bags at Pathfinder House where you can securely dispose of paper. Records can be deleted from a system either by the team who support the system or the provider.

### Whose responsibility is records management?

All of us.

# The Retention Schedule

We have a retention schedule that sets out what we have and how long we keep it for. It should also list where the information is and it is important that this is updated when we move information.

The Retention Schedule is attached to this policy.

If you become aware of a new legal requirement, or code of practice, with respect to a specific type of record then please let the Data Protection Officer ("DPO") know.

If you see that something is missing, then please let us know. This is a live document and can change as we collect new information.

The DPO will provide advice, guidance and training where necessary.

# Storing records

It is important that we have a few rules about storing records:

- We should know what records we hold and who they are about
- We should know where records are
- We should make sure they are secure and safe so we know who can access them
- We have someone who knows the above and keeps the schedule updated
- If we cannot find one then we have an audit trail of who accessed it last or what the last thing done was

# Accessing Records

When we give access to records then we should make sure that we know why someone has should access them. It means knowing that they have a genuine business reason to do so. Just because someone is interested does not mean that they have a reason.

If you hold paper copies then you should have a system in place for recording what file has been accessed or removed, by who and when. It should then be marked back as returned. A bit like a library book.

# Destroying records

Always take care when destroying information and make sure that it is ok to destroy.

If it has personal information in then check the retention schedule. If it doesn't then you should make certain that we can destroy it.

### Non personal information

This could be emails, letters, circulars or documents. It may not contain personal information but it may contain confidential or business sensitive material. You should make sure that it is not still needed for audit purposes and then destroy it securely in the same way as personal data described below.

### Hard copies of records

Paper records should be destroyed securely using the confidential  shredding cupboard. The authority has a shredding cupboard and shredding bags at Pathfinder House which are dealt with under a contract and ensures that the paper copies are shredded professionally. If you have large amounts then you should speak to the Data Protection Officer who will assist in identifying a way you can do this. If a company is storing them on our behalf then we will ask for a certificate of destruction.

Please keep a list of what has been destroyed, when and by who.

### Electronic files

All departments will have electronic records held on secure systems. Access to these will be restricted to those who have a legitimate requirement for access and this access will have specific security processes like usernames and passwords.

Systems and databases will be subject to any policies, corporately and at departmental level, which ensures routine back ups and contingency plans are in place to maintain the records.

Where a case is closed or a record is no longer needed, it will be subject to the appropriate retention period and will then be securely deleted by either the support team or provider.

# Changing the way we hold information

If any records are being transferred such as being scanned then the previous versions can be disposed of securely. You should discuss this with the DPO and consider whether a data protection impact assessment is needed. This would help you identify and manage any of the risks.

If the records are being transferred to another organisation, it is essential that secure transporting arrangements are in place regarding the transfer.  Contact the DPO for further information.

# Missing records

We hope that we won't lose records but sometimes it happens. If this happens then you must report this immediately following the process described in our guide to what to do if we have lost some data.

After any incident, you should review what happened and why so that we can change or update processes to prevent recurrence. The DPO will help with this and help implement changes where necessary.

.

# Who does what?

### All of us

We need to think about whether we need to keep information, what we keep, where we keep it and how long for.

### Data Protection Officer

The DPO will provide advice and guidance as well as maintaining the retention schedule, advising on timescales and helping ensure that information is kept securely.

### SIRO

The SIRO is the senior officer with responsibility for security, risk and data. This means that they will receive reports on any issues such as lost files, incorrect records, or insecure storage.

# Registers

The DPO will maintain the retention schedule.

# Monitoring and Review

This policy shall be reviewed annually after implementation.