ARUN DISTRICT COUNCIL

INFORMATION SECURITY POLICY

Records Retention and Disposal Policy

Document Owner	Liz Futcher Group Head of Council Advice & Monitoring Officer (Data Protection Officer)
Version	V2
Date	25.09.18
Document Classification	Unclassified

Records Retention and Disposal Policy

1. Introduction

The Council, in the course of carrying out its functions, will collect and record information from individuals, internal service areas and external organisations. These records can be in a number of forms, for example -

- Communications from customers;
- Emails and attendance notes;
- Financial Information, including invoices;
- Confidential information;
- Statements and reports;
- Legal documents, including contracts and deeds; or
- Information relating to various types of applications.

This information can be in both hard copy and electronic form.

The Council is required to have and to implement a records retention and disposal policy. For further information, please see the Lord Chancellor's Code of Practice on the Management of Records issued under the Freedom of Information Act 2000 section 46.

In addition, the Data Protection Act 2018 (**DPA**) provides that personal data processed for any purpose must be kept for no longer than is necessary for that purpose or purposes. This is reinforced by the General Data Protection Regulation (**GDPR**) which provides that personal data should be kept for no longer than is necessary and that time limits should be established by the controller for erasure or for a periodic review.

2. Purpose of this Policy

The key purpose of this Policy is to provide the Council with a framework which will govern decisions on whether a particular document should be retained or disposed of. This Policy will assist the Council in securing compliance with both the DPA and the GDPR in ensuring that personal data is kept for no longer than is necessary and to prevent the premature destruction of records that need to be retained for a specified period.

3. Scope of this Policy

Unless otherwise stated, or a business case can be presented, all documents should be destroyed six years' after they are no longer required or 'live' (in accordance with section 2 of the Limitation Act 1980). All times should be read as full financial years after closure or last entry.

All records should be reviewed at the end of the quoted time and considered both as individual records and in relation to departmental records as a whole, bearing in mind the purpose and value of their retention.

The spreadsheet that forms part of this Policy should be used as a guide and cannot be a definitive list. For any queries, please contact the Information Management Team.

4. Destruction of Records

Should there be a possibility of litigation, records and information should not be amended or disposed of until that threat has been removed.

Where records identified for disposal are destroyed, a register must be kept by each service area. The register should contain enough information to identify which and when records were destroyed. However, it should not contain any personal or sensitive personal data other than the name of the person who the details were about. An example table is below -

Name	What was destroyed	When was it destroyed

5. General Records

Some records may be destroyed in the usual course of business and will not need to be recorded in the register. This will usually include information that has been duplicated, of short-term value or can be deemed as unimportant. For example - telephone message slips, non-acceptance of invitations, out-of-date distributions lists, and working papers which lead to a final report.

Duplicated and superseded material may also be destroyed. This can include - address books and reference copies of annual reports.

6. Who this Policy applies to and their responsibilities

This Policy applies to everyone who has access to the Council's information.

All Staff are responsible for:

- following procedures and guidance for managing, retaining and disposing of records;
- only disposing of records in accordance with the requirements outlined within this Policy (should they have been given authority to do so);
- ensuring that any proposed divergence from this Policy is authorised; and
- reporting security incidents and breaches of this Policy as soon as possible via the Breaches Form found on SharePoint.

Team Leaders / Managers are responsible for ensuring:

- that this Policy is implemented within their team;
- record keeping systems and arrangement of records to enable identification of records due for disposal;
- records due for disposal are routinely identified and reviewed to ensure that they are no longer required;
- divergence from this Policy is authorised and that the Information Management Team are notified of any changes;
- staff dispose of records only in accordance with this Policy;
- records are disposed of appropriately considering their sensitivity, security classification and the media and format(s) in which they are held;
- ICT equipment and storage media are disposed of securely ensuring all records, data and information are removed in such a way that is not recoverable;
- records of potential historic interest or research value are identified and transferred with agreement to West Sussex County Council's Record Office; and
- where appropriate, a disposal register and the process of disposal is kept.

7. Compliance

This Policy will be officially monitored for compliance by the Corporate Management Team and by the Group Head of Council Advice and Monitoring Officer which may include random and scheduled checks.

8. Non-Compliance

The Council will take appropriate measures to remedy any breach of this Policy. In the case of a Council Officer, then the matter may be dealt with under the Council's disciplinary procedures.

A breach of this Policy can be defined as an event which could have, or has resulted in, loss or damage to the Council assets, or an event which is in breach of the Council's security policies and procedures.

9. Reviewing this Policy

A further review of this Policy will be concluded by the end of December 2019. Any changes will be highlighted to enable Officers to modify their practices.

Document Log		
Version	Date	Action/Revision
V1	130917	Approved by Full Council
V2	250918	Updated by Group Head under delegated authority to reflect requirements of Data Protection Act 2018