STRONGER together

Lewes District Council

EASTBOURNE Borough Council

Working in partnership with Eastbourne Homes

Document name:	Data Retention, Storage and Disposal Policy
Document type:	Policy

Authority(ies) covered:	Aligned
Responsible (Executive Lead):	Becky Cooke, Assistant Director of HR and Transformation
Accountable (Operational Lead):	Rachael Page Information Governance Manager
Version (e.g. first draft, final report):	V02 This version supersedes the version approved on 12.09.18 (CMT) and published on 19.09.18
Approved by:	Becky Cooke on behalf of CMT, 30.07.20
Date of publication:	August 2020
Revision due:	12 months after publication
Final Equality and Fairness Analysis (EaFA) report approved by:	Not applicable
Date final EaFA report approved:	Not applicable

Contents

1. ABOUT THIS POLICY

1.1 The corporate information, records and data of Lewes District Council and Eastbourne Borough Council ('the councils') are a valuable resource to us and are important to how we conduct business and manage employees.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our councils operate and to have information available when we need it. However, we should not and do not need to retain all data indefinitely. Retaining data too long can expose us to risk as well as be a cost to our councils.

1.3 This Data Retention, Storage and Disposal Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 The legal framework for this policy comprises:

(i) the General Data Protection Regulation ('GDPR'), in particular the data processing principles relating to data minimisation, storage limitation, and integrity and confidentiality – as defined in paragraph 2 below;

(ii) the Data Protection Act 2018 – Part 2 and associated schedules;

(iii) the Lord Chancellor's Code of Practice on the management of records, issued under section 46 of the Freedom of Information Act 2000; and

(iv) the Information Commissioner's Office ('ICO') guide to the GDPR principles on the processing of personal data.

Accordingly, this policy requires us to comply with the legislation and to have due regard to the Code of Practice and guide mentioned above.

1.5 Failure to comply with this policy can expose us to legal action by affected parties; and ICO enforcement action, which may consist of inspections, statutory notices and penalties. Non-compliance can also lead to adverse publicity, difficulties in locating and providing evidence when we need it and in running our business.

1.6 This policy has been agreed by the Corporate Management Team.

1.7 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. DEFINITIONS

In this policy, the following terms have the meanings given.

Data: all data that we hold or have control over and therefore to which this policy applies. 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. It applies to both personal data and non-personal data (as defined below). In this policy we refer to this information and these records collectively as "data".

Data Minimisation Principle: the requirement that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data Protection Officer: our GDPR article 37 designated Data Protection Officer who is responsible for advising on and monitoring compliance with that Regulation.

Disposable information: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention and Disposal Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Record Retention and Disposal Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Information Governance Manager: the Information Governance Manager is responsible for administering the data management programme, helping Senior Managers Forum implement it and related best practices, planning, developing, and prescribing data disposal policies, systems, standards, and procedures and providing guidance, training, monitoring and updating in relation to this policy.

Integrity and Confidentiality Principle: the requirement that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised. It also applies to data from which the identity of an individual permanently removed.

Personal data: any information relating to an identified or identifiable living person; an identifiable living person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Identification may be from that data alone or in combination with

other identifiers we possess or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Records: information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or the transaction of business[1].

Record Retention and Disposal Schedule: the schedule attached at Annex A of this policy which sets out retention periods for our formal or official records[2].

Storage Limitation Principle: the requirement that personal data is kept for no longer than is necessary for the purposes for which it is processed.

3. SCOPE OF POLICY

3.1 This policy covers all data that we hold or have control over, whether produced or received, and in any format. 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. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

3.2 This policy applies to the councils' members, all its employees and all its business partners (such as contractors) who create and/or use records of the councils.

3.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

3.4 This policy incorporates the councils' policy – set out in Annex B – on the filing and storage of electronic information; this determines where and how such information should be stored.

4. GUIDING PRINCIPLES

4.1 Through this policy and our data retention practices, we aim to meet the following commitments:

- We manage the councils' data in accordance with applicable laws, codes of practice and regulatory guidance.

[1] This mirrors the definition given by the relevant British Standard: ISO15489-1:2201.
[2] This Schedule adopts the format specified by LG Inform Plus and Kent County Council

- We comply with our data protection obligations, in particular the principles relating to data minimisation, storage limitation, and integrity and confidentiality.

- We handle, store and dispose of data responsibly and securely.

- We create and retain data where we need this to run our councils effectively, but we do not create or retain data without good business reason.

- We allocate appropriate resources, roles and responsibilities to data retention.

- We regularly remind employees of their data retention responsibilities.

- We regularly monitor and audit compliance with this policy and update this policy when required.

5. ROLES AND RESPONSIBILITIES

5.1 The **sponsor** of this policy is the Assistant Director of HR and Transformation, whose role is (a) to ensure and monitor compliance with the policy, and (b) to ensure appropriate resources are available to support policy implementation.

5.2 **All employees** must comply with this policy, the Record Retention and Disposal Schedule, any communications suspending data disposal and any specific instructions issued by or on behalf of a member of the Corporate Management Team. Failure to do so may subject us, our employees and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary measures. It is therefore the responsibility of everyone to understand and comply with this policy.

5.3 **Senior Managers Forum** will–

- act as information asset owners and take the lead for records management issues specific to their service area

- develop and publish service-specific procedures in line with this policy

- ensure their staff follow all procedures (service-specific and council-wide) that implement this policy

5.4 The **Information Governance Manager** is responsible for–

- reviewing and maintaining this policy;

- advising Senior Managers Forum on the exercise of their responsibilities above;

- supporting staff in the interpretation and application of the policy; encouraging compliance

- planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and

- providing guidance and training in relation to this policy.

- identifying the data that we must or should retain, and determining, in collaboration with Legal Services, the proper period of retention.

5.5 The **Head of ICT** is responsible for developing the IT systems and capability for (i) the retention and storage of electronic data; and (ii) the destruction of electronic records whose retention period has expired, and ensuring compliance.

5.6 The **Data Protection Officer** (DPO) is responsible for advising on and monitoring our compliance with the GDPR. Our DPO works with our Information Governance Manager on the retention requirements for personal data and on monitoring compliance with this policy insofar as it applies to personal data.

5.7 **Internal Audit** is responsible for monitoring and reporting on compliance with this policy.

6. TYPES OF DATA

6.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention and Disposal Schedule at Annex A. This may be because we have a legal requirement to retain the data, or because we may need it as evidence of our transactions, or because it is important to the running of the councils. See paragraph 7.1 below for more information on retention periods for data of this type.

6.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention and Disposal Schedule. Examples may include:

- duplicates of originals that have not been annotated

- preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record

- books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the councils and retained primarily for reference purposes

- spam and junk mail.

For more information on how to determine retention periods for this type of data, see paragraph 7.2.

6.3 **Personal data.** Both formal or official records and disposable information may contain personal data. For information about retention periods for personal data, see paragraph 7.3.

6.4 **Confidential information belonging to others**. Any confidential information that an employee may have obtained from a source outside of the councils, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted if received via the internet.

7. RETENTION PERIODS

7.1 **Formal or official records.** Data that is part of any category listed in the Record Retention and Disposal Schedule must be retained for the period indicated in that Schedule. A record must not be retained beyond the period indicated unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Information Governance Manager.

7.2 **Disposable information**. The Record Retention and Disposal Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value, it should be securely disposed of.

7.3 **Personal data.** As explained above, we must retain personal data for no longer than is necessary for the purposes for which it is processed. Where data is listed in the Record Retention and Disposal Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data.

7.4 **What to do if data is not listed in the Record Retention and Disposal Schedule.** If data is not listed in the Record Retention and Disposal Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Schedule, or if you are unsure, please contact the Information Governance Manager.

8. STORAGE, BACK-UP AND DISPOSAL OF DATA

8.1 **Storage.** To comply with the integrity and confidentiality principle, our data must be stored in a safe, secure, and accessible manner, using appropriate technical or organisational measures. The councils' policy on the filing and storage of electronic data is set out in Annex B.

8.2 **Destruction**. Except in the circumstances specified in paragraph 7.1 (a "valid business reason") or 9.1, formal or official records must not be kept beyond the period given in the Retention and Disposal Schedule and, once the retention period has elapsed, the data must be destroyed securely, if appropriate by automated means.

8.3 The councils will, subject to financial concurrence and ICT and operational viability, seek to implement automated disposal modules in order to maximise the speed and effectiveness of electronic data destruction at the appropriate times.

8.4 The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be in accordance with any policy, procedure or guidance issued by the Head of ICT.

8.5 Take care with print outs. At the office, you can use shredders or confidential waste bins. When working from home, you're unlikely to have that facility. Follow any specific guidance the Council issues or safely store print outs until you can take them into the office and dispose of them securely.

8.6 We may provide storage for third party companies. Any documents that are stored for third parties is not the responsibility of the council to ensure that data is destroyed once the retention period has passed.

8.7 The destruction of data must stop immediately upon notification from Legal Services that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see 9.1). Destruction may begin again once Legal Services lifts the requirement for preservation.

9. SPECIAL CIRCUMSTANCES

9.1 **Preservation of documents for contemplated litigation and other special situations.** Officers should note the following general exception to any stated destruction schedule: if you believe, or Legal Services informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until Legal Services determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention

and Disposal Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

9.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact Legal Services.

9.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as business re-organisation or transformation, or the replacement of our information technology systems.

10. WHERE TO GO FOR ADVICE AND QUESTIONS

10.1 **Questions about the policy.** Any questions about retention periods relevant to your function should be raised with your Head of Service. Any questions about this policy should be referred to the Information Governance Manager (rachael.page@lewes-eastbourne.gov.uk), who is in charge of administering, enforcing, and updating this policy.

11. POLICY BREACH AND AUDIT

11.1 **Reporting policy breaches.** We are committed to enforcing this policy. The effectiveness of our efforts, however, depends largely on rapid identification and response. Any councillor or officer who believes that they or someone else may have breached this policy should report the incident immediately to their line manager (or, for councillors, the Committee and Civic Services Manager). If any officer or councillor believes that, on reporting a breach, the matter has not been acted upon properly, they should raise the matter with the Information Governance Manager. If officers and councillors do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

11.2 No one will be subject to, and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

11.3 **Audits**. Our Information Governance Manager will periodically review this policy and its procedures (including, where appropriate, by taking outside legal or auditor advice) to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

12. OTHER RELEVANT POLICIES

12.1 This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- ICT policies
- Data protection policy
- Disaster Recovery Plan
- Any other security and data related policies.

RECORD RETENTION AND DISPOSAL SCHEDULE

The Schedule can be found here:

https://www.councilhub.net/policies/?opentab=3&esprrenderhostpagestructuredisplayrendererectl96fe6496-ddc9-4a49-979e-3a53eeb163eactl00innerrenderer96fe6496-ddc9-4a49-979e-3a53eeb163eaesctl54861230-d032-4db1-b953-9e701182f566ctl00innerrenderer54861230-d032-4db1-b953-9e701182f566esctl49e4dc13-4e46-4fef-92d5-4ae241cfb2a2pager_p=2

The rest of this page is blank

ANNEX A POLICY ON FILING AND STORAGE OF ELECTRONIC INFORMATION

This policy is set against the background of data protection legislation but is separate from the councils' Data Protection Policy. It also sits alongside the IT acceptable use policy, the Records Management Policy and the Retention and Disposal Schedule.

As well as compliance with data protection legislation, this policy aims to ensure that all information necessary to carry out work is held in suitable locations where it is accessible to all relevant staff. Also, it aims to help free up space on servers by backing up the requirements of the Retention and Disposal Schedule.

Electronic information is stored in many different locations and, unlike paper filing, it is not so obvious how much is being held. Over time information is filed and forgotten and, with the strain on staff resources, time is not allocated to weeding and deleting this information. However, this puts the council in breach of its own Retention and Disposal Schedule as well as data protection legislation.

In addition, work information has been filed in locations where it is not accessible to other staff who may need access to it for work purposes, or it is held in folders that are not adequately named therefore making the information harder to find by other staff.

This policy will set out where work information should be held so that the authority can comply with data protection legislation, ensure that the council's retention and disposal policy is adhered to ensure and that all work information is readily accessible to all relevant staff.

Retention Periods

It is important that any information is stored for no longer than is required. At no time should information be held just in case it may be needed. If the information contains personal information then this would be in contravention of data protection legislation. However, retaining unnecessary data/information causes issues with data storage and there is only a finite amount of this on servers. Electronic filing must therefore be kept at a minimum. The Retention and Disposal Schedule on The Hub (intranet) gives the retention periods for different types of information held and this should be the adhered to. However, as a general rule, if there is no need to retain information then it should be deleted as soon as possible.

Where information is stored

All work must be stored on shared drives. This is in order that anyone necessary can access the work. If required it is possible to limit who can access any folder but this should only be necessary where there is a valid reason for other members of a team not to be able to access the documents – e.g. staff appraisals, sickness records etc. Access must not be limited to just one member of staff as doing so effectively makes the folder a personal folder.

Personal drives

All employees are set up with a personal drive – this should only be used for information that is personal to you. It must not be used for anything that is to do with work. All work, even if it is just a draft document, must be saved on a relevant shared folder. If a member of staff leaves, goes on sick leave or is absent for any reason there is no automatic right of access to

their personal drive. Therefore any piece of information that is required to carry out work must not be retained on personal drives.

Outlook inboxes and folders

This should be dealt with in the same way as personal drives. If a member of staff leaves, goes on sick leave or is absent for any reason there is no automatic right of access to their Outlook folders. Any emails that need to be stored for use in work must be stored on relevant shared folders where they can be accessed by other members of the team. The only exception is where the Outlook folder is one that is already a shared folder. Where inboxes are not shared then work emails must be saved on shared folders outside of Outlook.

While this may sound onerous it must be remembered that emails can contain personal data and if they are held in Outlook then it is extremely unlikely that they are being deleted in accordance with retention and disposal requirements. It also means that the emails will be readily accessible to other staff who may require the information for work purposes, particularly if the person who received the email is absent.

N.B. When emails are saved outside of Outlook it is still possible to open them, forward and respond to them as though they were in Outlook.

Hard drive

Information must not be routinely saved onto hard drives (and as documents on desktops). There are times when this is reasonable (e.g. when needing to work on something when there will be no internet connection) but this must be only temporary.

Naming conventions

When naming folders, thought needs to be given to using a name that means something to other users. Personally named folders on shared drives must be discouraged even if it is accessible to other staff. If folders are named after a member of staff it gives no indication of what work is held within that folder. All work should be held in folders that are named in a way that clearly indicates what is held in there.

Where possible folders and/or documents should contain a year as well as theme e.g. staff appraisals/17-18, as this will then allow easy identification for deleting information when the set retention period is reached.

For more information on how to name documents please use the Document Naming Protocol that can be found on The Hub under joint policies.

What should managers do?

Managers need to ensure that their staff do not retain work information on personal drives, personal Outlook folders or on hard drives. They should also ensure that all information is retained in accordance with the Retention and Disposal Schedule. This should be routinely raised at 1-2-1s and team meetings.

What should Senior Managers Forum do?

Senior Managers Forum should ensure that their managers are aware of the requirements of this policy and get assurance from them that it is being observed. Senior Managers Forum will be asked to give assurance of this on the annual Managers' Assurance Statements.

IT

IT will delete any email account and personal folder for any leavers after a set retention period. They will delete any historical personal folders for staff who have already left the employment of the councils.

Internal Audit

Internal Audit will confirm that data retention periods are being adhered to, and that data is held in accordance with this document, in every audit review undertaken.