



Data Retention Audit 23-24

FINAL REPORT

Jeremy Todd and Laura Hutchison December

2023

Distribution List:

Diane Shepherd (Chief Executive), John Ward (Director of Corporate Services), Louise Rudziak (Director of Housing & Communities), Andrew Frost (Director of Planning & Environment), Jane Hotchkiss (Director of Growth & Place), Helen Belenger (DM- Financial Services), Joe Mildred (DM- Business Support) , Pam Bushby (DM- Communities & Wellbeing), Sarah Peyman (DM– Growth & Place), Laurence Foord (DM - Communications, Licences & Events), Kevin Carter (DM- Contract Services), Nicholas Bennett (DM- Legal & Democratic Services), Fjola Stevens (DM- Development Management), Alison Stevens (DM- Environment and Health Protection), Victoria McKay (DM- Property & Growth), Kerry Standing (DM- Revenue's, Benefits & Housing), Tania Murphy (DM– Place), Tony Whitty (DM- Planning Policy), David Cooper (Group Accountant– Revenue & Corporate financial Management)

Contents

Page

1) Executive Summary:

- i) Introduction 3 ii) Overall audit opinion 3 iii) Summary of findings 4-5

2) Exceptions raised

- i) Key for risk rating of exceptions 6
ii) Detailed exceptions 7-14

iii) 1) Executive Summary

i) Introduction

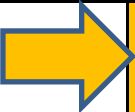
This audit was carried out as part of the agreed audit plan for the 2023-2024 financial year. Audit testing has been restricted to areas that have been assessed as high risk by Internal Audit.

Audit testing has been carried out on the following objectives to ensure that:

- **Objective 1 - There are clear and current policies and processes in place across Chichester District Council that supports data retention legislation.**
- **Objective 2 - Manual Data is retained, controlled, archived, or destroyed as per policy.**
- **Objective 3 - Electronic Data is retained, controlled, archived, or destroyed as per policy across all platforms within Chichester District Council.**

ii) Overall audit opinion

The overall audit opinion is based solely on testing carried out and discussions held during the course of the audit.

	Levels	Description/Examples
	No Assurance (Critical Risk Exceptions)	Major individual issues identified or collectively a number of issues raised which could significantly impact the overall objectives of the activity that was subject to the Audit
	Limited Assurance (High Risk Exceptions) Authority	Control weaknesses or risks were identified which pose a more significant risk to the
	Reasonable Assurance (High Medium Risk Exceptions) significant risks to the Authority	Control weaknesses or risks were identified but overall the activities do not pose or
	Assurance (Low Risk/Improvement Exceptions)	No issues or minor improvements noted within the audit but based on the testing conducted, assurance can be placed that the activity is of low risk to the Authority

iii) Summary of findings

Objective 1: To ensure that there are clear and current policies and processes in place across Chichester District Council that supports data retention legislation –Reasonable Assurance

Two low risk and one medium risk exception were raised as a result of this testing.

The current data policy in place was found to be concise and appropriate but changes in GDPR legislation and changes within service areas of CDC mean that the policy requires reviewing and updating.

Each appropriate service area has their own Service Data Protection policy on the external website - excluding Housing which is missing. All service areas have sections in the Register of Data Processing covering the data they have plus guidance within the CDC Retention Scheme document.

We completed a risk Matrix for the manual data across the council following a top line assessment of all the service areas, the data they handle, its level of sensitivity, frequency they would handle this data and the controls the service area had in place at the time of our review. From these the highest risk areas were – Rev's Ben's and Housing scoring 14 (out of 15), Business Support (HR) on 12 (out of 15) and then 2 services areas were on 11 (out of 15) which were Growth and Communities, and Events.

Within the register of data processing there is no recorded protocol for the destruction of electronic records, and this was seen with the amount of data held on our internal systems when reviewed for all the service areas. There is guidance on the retention, but this is not clearly stated as applicable to both manual and electronic, there is nothing to support the removal process.

See Ex 1.1, 1.2 & 1.3 for full testing details.

Objective 2: To ensure that manual data is retained, controlled, archived, or destroyed as per policy. - Limited Assurance Three high risk exceptions were raised as a result of this testing.

We completed a risk Matrix for the manual data across the council following a top line assessment of all the service areas, the data they handle, its level of sensitivity, frequency they would handle this data and the controls the service area had in place at the time of our review.

In comparison with the retention document- the standard of compliance to the data retention documents varied, but all service areas need to review their compliance, remove data outside the scope of retention and destroy unrequired data following destruction policy guidelines.

Key Control for manual data was an issue for both HR and the strong room records, plus key control by facilities in general needs to be reviewed. There was confusion and lack of clarity around who held keys and where for the strong rooms and other controlled rooms.

Documents are held unsecured in car parking storage areas, the Depot, plus documents held in offices across CDC and around service area locations. During the tour of the CDC building, we also discovered an external dept using our committee room facilities as court areas - having unsecured personal data. Which if discovered would impact directly on CDC's reputation.

No records of archiving or destruction were seen on the shared drive from our checks and only one service area could refer us to this.

See Ex 2.1, 2.2 & 2.3 for full testing details.

Objective 3: To ensure that electronic data is retained, controlled, archived or destroyed as per policy across all platforms within CDC - Assurance

Two low risk exceptions were raised as a result of this testing.

The council uses the following systems - Iken, Northgate, Homemove, Uniform, Chipside, Exacom, Pentana, Civica, Itrent, WRAPP, as well as numerous shared drives. The data retention policy refers to the control of data which includes both manual and electronic, but the data processing document for the majority of service areas clearly states that “there is no protocol” for the removal or anonymisation of data held on these systems. At present the only systems with an anonymization of data function is the Uniform and Iken systems. But within Uniform this is not being utilised by all the service areas using it. Work is in progress around ensuring this function is built into all future procurement conversations for all platforms.

We completed a review of data held on the Shared drive within the council data is held on all systems and shared drives over and above the retention policy guidelines but access control to these systems is well managed and monitored by IT access restrictions. A scan of the disk space by the ICT Manager highlighted 3.9 million S-drive files are currently held across the council. The holding of excess data has a financial impact currently in back-up time and disk space used.

See Ex 3.1 & 3.3 for full testing details.

Overall assurance level – Limited Assurance

There were Four low, one medium and three high risk exceptions raised in total and therefore IA can give Limited assurance that the area is of high risk to the Authority.

Key for risk rating of exceptions:

Priority Level	Description
-----------------------	--------------------

Critical Risk	Control weakness that could have a significant impact upon not only the system function or process objectives but also the achievement of the organisation’s objectives in relation to: <ul style="list-style-type: none"> □ The efficient and effective use of resources □ The safeguarding of assets □ The preparation of reliable financial and operational information □ Compliance with laws and regulations And corrective action needs to be taken immediately.
High Risk	Action needs to be taken to address significant control weaknesses but over a reasonable timeframe rather than immediately. These issues are not “show stopping” but are still important to ensure that controls can be relied upon for the effective performance of the service or function. If not addressed, they can, over time, become critical. An example of an important exception would be the introduction of controls to detect and prevent fraud.
Medium Risk	These are control weaknesses that may expose the system function or process to a key risk but the likelihood of the risk occurring is low.
Low Risk - Improvement	Very low risk exceptions or recommendations that are classed as improvements that are intended to help the service fine tune its control framework or improve service effectiveness and efficiency. An example of an improvement recommendation would be making changes to a filing system to improve the quality of the management trail.

Exception no 1.1- A clear and current data retention policy is in place to cover all service areas of the CDC.
Risk rating: Low
Findings

On the Chichester District council's external website there is a Data Protection and Freedom of Information page, this provides public information on the Freedom of Information Act 2000, plus easy access for the public to make a request for their information, there is also:

Information for the register of Data Processing and Retention Scheme, this includes links to a register of Data Processing Spreadsheet (August 2023) and a Chichester District Council retention scheme word document (Version 8 Sept 2022) alongside these documents there is information around the Data Protection Act 2018 and General Data Protection Regulations. The Six data protection principles are listed explaining how Chichester Council follow these in relation to collecting, processing, and storing individuals' personal data and that the data controller is responsible for complying with these principles. It also explains the processes around Data matching around the Local Audit and Accountability Act 2014. This section then includes a request for Disclosure of personal information document.

At the bottom of the page is the Service data protection policies - this is each individual service area's policy around data they hold, what they hold and how this is used, plus customers rights and multiple methods for contact. The Service area information is labelled using multiple different headers, this is due to a decision at SLT level to give the responsibility to produce this information to each individual Division Manager with Support only from Data Protection Officer (DPO) and his team.

The CDC Retention Scheme Document itself was last updated 30/9/22. This policy is comprehensive, clear and covers all the service areas, but although this document was updated in 2022, due to the changes around the UK leaving the European Union, compliance to GDPR and changes within service areas within the CDC, this document does need to be reviewed and redrafted. In its current form it is still relevant and appropriate.

Alongside the CDC Retention scheme document on the external website is a spreadsheet, The Register of Data processing (August 2023). This spreadsheet gives detailed information by each service area covering the data we hold with regards to Personal data, Sensitive Data, and data for those under 16 years old, this covers what data we hold, where we hold it, who accesses it, its format, how long it is kept, what's on it, and what we do with it once used. This is a comprehensive spreadsheet giving detailed information, but some areas of it are confusing with regards to exactly which service area or Dept this refers to Older reference material was found on the internal website - Intranet - Retention Guidelines - 2017 - this has now been removed, and Data protection Policy - 2007. which was in the ICT section of the intranet.

At present the Register of Data Processing states for the majority that 'there is no protocol' with regards to the destruction of electronic data. - following discussions with the DPO. this is addressed in detail within the electronic data section of this audit, but a decision needs to be made by each individual service area in relation to the data they hold and the risk level of this data.

A full review of the policy highlighted that there is no reference to the use of lockers for the storage of data or data in relation to homeworking and the controls required if manual or electronic data is required away from the office. (IT policy 2018)

Risks and consequences

That the Council is not following the legislation in relation to Data Retention. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation.

Agreed action

Officer responsible and by when

Policy requires reviewing and updating due to changes in service areas and changes in UK's compliance to GDPR.	Data Protection Officer – August 2024
Data retention in relation to Lockers and home working to be reviewed.	Data Protection Officer – August 2024

Exception no 1.2 The data retention policy is appropriate in line with current legislation.	
Risk rating: Low	
Findings	
As above the policy was updated 30/9/22 - This policy is comprehensive, clear and covers all the service areas, but although this document was updated in 2022, due to the changes around the UK leaving the European Union, compliance to GDPR plus also changes within service areas within CDC this document does need to be reviewed and redrafted. In its current form it is still relevant and appropriate	
Risks and consequences	
That the Council is not following current legislation in relation to Data Retention. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation	
Agreed action	Officer responsible and by when
Policy requires reviewing and updating due to changes in service areas and changes in UK's compliance to GDPR	Data Protection Officer – August 2024

Exception no 1.3 There are processes to follow for each service area in relation to the data they handle.	
Risk rating: Medium	
Findings	

Each appropriate service area has their own Service Data Protection policy on the External website - excluding Housing which is missing. All service areas have sections in the Register of Data Processing covering the data they have plus guidance within the CDC Retention Scheme document.

We completed a risk Matrix for the data handled across the council following a top line assessment of all the service areas, the data they handle and the level of sensitivity of this data and the frequency they would handle this data and the controls the service area had in place at the time of our review. From these the highest risk areas were – Rev’s Ben’s and Housing scoring 14 (out of 15), Business Support (HR) on 12 and then two service areas were on 11 which are Growth and Communities, and Events. This was based on Paper documents held. Within the register of data processing there is no recorded protocol for the destruction of electronic records, and this was seen with the amount of data held on our internal systems when reviewed for all the service areas. There is guidance on the retention, but nothing to support the removal process.

Risks and consequences

That individual service areas do not have clear processes to follow to enable them to meet required legislation guidelines. Risk of Fines if legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation

Agreed action

Review the data retention spreadsheet and the protocol for the removal of electronic data to adhere to retention guidance.

Review the external websites data protection policies and ensure all appropriate service areas have a policy present.

Officer responsible and by when

Data Protection Officer and all Divisional Managers – August 2024

Data Protection Officer and all Divisional Managers where appropriate – August 2024

Exception no 2.1 - Manual data across the council is retained in line with policy.

Risk rating: High

Findings

We completed a risk Matrix for the manual data handled across the council following a top line assessment of all the service areas, the data they handle and the level of sensitivity of this data and the frequency they would handle this data and the controls the service area had in place at the time of our review. We also completed a review of data held on the Shared drive within the council. In comparison with the retention document- the standard of compliance to the data retention documents varied, but all service areas need to review their compliance, remove data outside the scope of retention and destroy unrequired data, this applies to both manual and electronic

Risks and consequences

Manual data is not retained as per policy and GDPR legislation is breached. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation	
Agreed action	Officer responsible and by when
All service areas required to comply with data retention guidance for manual documentation or have measures in place to address this going forward.	Data Protection Officer and all Divisional Managers – August 2024
All Divisional Managers to be briefed on findings from the audit in relation to Manual and Electronic data held in their service areas to support compliance.	Internal Audit and all Divisional Managers. – Completed

Exception no 2.2 - Access to manual data across the council is controlled as per the council policy.	
Risk rating: High	
Findings	
Key Control for manual data was an issue for both HR and the strong room records, plus key control by facilities in general need to be reviewed. There was confusion and lack of clarity around who held keys and where for the strong rooms and other controlled rooms.	
Documents are held unsecured in car parking storage areas, the Depot, plus documents held in offices across CDC and around service area locations in our tour of the CDC building we also discovered an external dept using our committee room facilities as court areas - having unsecured personal data. Which if discovered would impact directly on CDC's reputation.	
Risks and consequences	
Manual Data is breached as access is not controlled across the council. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation	
Agreed action	Officer responsible and by when

<p>All service areas to review access controls for documentation to bring them in line with the retention policy to ensure security of data.</p> <p>Action taken to ensure all EPH tenants (CAB & Courts) are reminded of their responsibilities around data retention and data handling e.g., court documents.</p> <p>Review the control and organisation of keys held by facilities and their security.</p> <p>To assist Service areas with document management with a managed and updated record of all lockable cupboards within East Pallant house so that any not required can be reallocated to Service areas requiring them.</p>	<p>Data Protection Officer and all Divisional Managers – August 2024</p> <p>Facilities Manager – August 2024 -Action taken by FM – Email communication with Court Delivery Manager. Audit to review.</p> <p>Facilities Manager – August 2024</p> <p>Facilities Manager – August 2024</p>
--	--

<p>Exception no 2.3 - Manual data is archived or destroyed as per policy. Risk rating: High</p>	
<p>Findings</p>	
<p>No records of archiving or destruction were seen on the shared drive from our checks and only one service area could refer us to this.</p> <p>There were gaps in the logbook for documents signed in and out of the strong room. Box numbers are needed on log, or it is impossible to find where the document belongs. There is a printed list of full box and deeds list on the shared drive. Plus, an updated printed version held within legal in case the system goes down.</p> <p>Other service areas - many were unaware of documents held in the depot and/or storage areas around the council offices. - Land Charges have good records in place, HR was unaware confidential data was still held at depot.</p>	
<p>Risks and consequences</p>	
<p>Manual Data is breached as access is not controlled across the council. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation</p>	
<p>Agreed action</p>	<p>Officer responsible and by when</p>

All service areas required to comply with data retention guidance for manual documentation in relation to archiving and destruction, where possible, or have measures in place to address this going forward.	Data Protection Officer and all Divisional Managers – August 2024
---	---

Exception no 3.1 - Electronic data across the council is retained in line with policy.	
Risk rating: Low	
Findings	
<p>The council uses the following systems - Iken, Northgate, Home finder, Uniform, Chipside, Exacom, Pentana, Civica, Itrent, WRAPP, as well as numerous shared drives. The data retention policy refers to the control of data which includes both manual and electronic, but the data processing document for most service areas clearly states that “there is no protocol” for the removal or anonymisation of data held on these systems. At present the only system with an anonymization of data function is the Uniform system. But this is not being utilised by all the service areas using Uniform. Work is in progress around ensuring this function is built into all future procurement conversations for these platforms.</p> <p>Data is held on all systems and shared drives over and above the retention policy guidelines. A scan of the disk space by the ICT Manager highlighted 3.9 million S-drive files are currently held across the council. The holding of excess data has a financial impact currently in back-up time and disk space used.</p>	
Risks and consequences	
Electronic data is not retained as per policy and GDPR legislation is breached. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation	
Agreed action	Officer responsible and by when

Actions to be put in place to comply with the data retention policy for electronic data held on all internal systems. (Where available)	Data Protection Officer and all Divisional Managers – August 2024
All Divisional Managers to be briefed on findings from the audit in relation to Manual and Electronic data held in their service areas to support compliance.	Internal Audit and all Divisional Managers. – Completed
All service areas to be provided with a break down on data held on the shared drive for their area.	Internal Audit and all Divisional Managers. – Completed

Exception no 3.3 - Electronic Data is archived or destroyed as per policy.	
Risk rating: Low	
Findings	
The council uses the following systems - Iken, Northgate, Home finder, Uniform, Chipside, Exacom, Pentana, Civica, Itrent, WRAPP, as well as numerous shared drives. The data retention policy refers to the control of data which includes both manual and electronic, but the data processing document for most service areas clearly states that “there is no protocol” for the removal or anonymisation of data held on these systems. At present the only system with an anonymization of data function is the Uniform system. But this is not being utilised by all the service areas using Uniform. Work is in progress around ensuring this function is built into all future procurement conversations around these platforms.	
Data is held on all systems and shared drives over and above the retention policy guidelines. A scan of the disk space by the ICT Manager highlighted 3.9 million S-drive files are currently held across the council. The holding of excess data has a financial impact currently in back-up time and disk space used.	
Risks and consequences	
Electronic data is not retained as per policy and GDPR legislation is breached. Risk of Fines if Legislation has not been followed, reputational risk if customers data is not retained as policy and Legislation.	
Agreed action	Officer responsible and by when

Actions to be put in place to comply with the data retention policy for electronic data held on all internal systems.

Data Protection Officer and all Divisional Managers – August 2024