Internal Audit Report

Pension Administration - Information Governance (2020/21)

Final Report

Assignment Lead: Elaine Laycock, Principal Auditor
Assignment Manager: Mark Winton, Audit Manager
Prepared for: East Sussex County Council
Date: May 2021

Internal Audit Report – Pension Administration - Information Governance (2020/21) Detailed Findings

Draft Report Distribution List

- Paul Punter, Head of Pensions Administration
- Sian Kunert, Head of Pensions
- Sarah Turner, Senior Information Governance Officer

Final Report Distribution List

As draft report with the inclusion of the following:

- Phil Hall, Interim Chief Operating Officer
- Ian Gutsell, Chief Finance Officer
- Matt Scott, Chief Technology Officer
- Heidi Judd, Data Protection Officer
- Nikki Wilkins, Head of Strategy & Engagement
- Pension Board
- Pension Committee

This audit report is written for the officers named in the distribution list. If you would like to share it with anyone else, please consult the Chief Internal Auditor.

East Sussex County Council - Internal Audit Key Contact Information

Chief Internal Auditor: Russell Banks, ☎ 07824362739, ✉ russell.banks@eastsussex.gov.uk
Audit Manager: Mark Winton, ☎ 07740517282, ✉ mark.winton@eastsussex.gov.uk
Anti-Fraud Hotline: ☎ 01273 481995, ✉ FraudHotline@eastsussex.gov.uk

Internal Audit Report – Pension Administration - Information Governance (2020/21) Detailed Findings

1. Introduction

1.1. The Council (East Sussex County Council) is the designated statutory administering authority of the East Sussex Pension Fund. As at 31 March 2020, the Fund comprised 128 scheme employers with 23,835 active, and 31,622 deferred, scheme members. The governance of the Fund is the responsibility of the East Sussex Pension Committee, and the Pension Board, supported by the Chief Finance Officer for East Sussex County Council.

1.2. The Council, as the administering authority and data controller for the fund, hold significant volumes of personal data in order to accurately administer and manage the fund and also to satisfy the legal obligations outlined within the Local Government Pension Scheme Regulations (LGPS). This can include, but is not limited to, names, addresses, contact telephone numbers and email addresses but also information relating to dependents/nominated beneficiaries and, in some cases, special category data such as health status.

1.3. Failure to adequately protect scheme member data can result in a personal data breach. Under the General Data Protection Regulations certain personal data breaches are required to be reported to the Information Commissioner's Office (as supervisory authority). These breaches can include, but are not limited to, access by unauthorised individuals and the sending of personal data to incorrect recipients. The Council is responsible to deciding on whether the breach needs to be reported based upon the risk to the individual's 'rights and freedoms'.

1.4. The Council has produced and published a Memorandum of Understanding regarding Compliance with Data Protection Law in relation to the LGPS which is available on the Council's website. This document details the basis on which data will be shared between interested parties and the administering authority's expectations of scheme employers.

1.5. This review is part of the agreed revised Internal Audit Plan for 2020/21.

1.6. This report has been issued on an exception basis whereby only weaknesses in the control environment have been highlighted within the main body of the report.

2. Scope

2.1. The purpose of the audit was to provide assurance that controls are in place to meet the following objectives:

- Employees within the pension service are aware of their roles and responsibilities under the relevant legislation including, the General Data Protection Regulations, Data Protection Act and Local Government Pension Scheme Regulations in relation to the security and ownership of data.

- There are clear processes in place that are instigated should there be a suspected data protection breach.

- The Council have issued a Privacy Notice which is available to all scheme members and pensioners and outlines the information they hold and how it is safeguarded.

- The Pension Fund systems (including the employer portal) are maintained to the required standard and system administration exercises and updates are completed by appropriately qualified officers.

- The “Principle of Least Privilege” is adopted for all pensions fund systems and information sources meaning that users are given the minimum levels of access/permissions needed to perform their role/responsibilities.

- Data sharing agreements are in place with all relevant parties.

- Data Protection system requirements are being incorporated into the procurement process for the new sovereign Pension Fund system.

3. Audit Opinion

3.1. **Reasonable Assurance is provided in respect of Pension Administration - Information Governance (2020/21)**. This opinion means that most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives. *Appendix A provides a summary of the opinions and what they mean and sets out management responsibilities.*

4. Basis of Opinion

4.1. At the time of this review the council was in the process of returning the Pensions Administration service back to sovereign control within Finance, having previously been part of the Orbis cross authority Business Operations service. As a result of this a new service structure has been created, a number of administrative staff have TUPE transferred to the council and a recruitment exercise is underway for the remaining vacant posts.

4.2. The council has recently entered into a contract for the provision of a sovereign Pension Fund administration system and is in the process of a data migration exercise to transfer scheme member data to the newly procured system. An internal audit review of the data migration process has been commissioned and is underway. This data migration review is focussing on risks relating to data mapping, the security and integrity of data and system testing and will be reported separately.

4.3. Under the Orbis Pensions Administration service, Surrey County Council employees have held responsibilities relating to system administration including, but not limited to, system upgrades, patches and user administration. We understand that the sovereign team, with support from officers from IT & Digital, will take responsibility for these areas for the new system and work, as this arrangement is in its infancy we have not sought to provide any assurance over these arrangements at this time.

4.4. During this review we were notified of a personal data breach relating to the transfer of data between the payroll and pensions teams using the iConnect module. This breach was investigated by the Head of Pensions Administration with remedial action taken and safeguards put in place to highlight any further recurrence of this issue. We note that this was not recognised as a personal data breach by the Pensions Officer handling the initial complaint and there is a risk therefore that there may have been other potential breaches that have not been reported or investigated as required.

4.5. Corporate policies detailing the action to be taken following reports of potential data breaches are clear and available to all employees via the council's intranet. In addition to this clear records are maintained on the corporate breaches log.

4.6. Should a potential breach be reported, support is available to service managers and affected employees provided by named individuals within the Information Governance team.

4.7. A breaches log (including regulatory breaches) is maintained within the Pension Administration service and reported to the Pension Committee on a quarterly basis.

4.8. We found that data subjects have not been provided with access to a Summary Privacy Notice and that the Full Privacy Notice is incomplete and therefore not compliant with General Data Protection Regulations. In addition to this we note that there are discrepancies between the length of time data is retained and the information provided to data subjects regarding data retention.

4.9. Testing identified that the council and fund websites contain out of date policy documents. This issue has been raised in the review of Pension Fund - Compliance with Regulatory Requirements 2020/21 and therefore is not included further within this report.

4.10. Through a review of recently advertised job descriptions we note that no reference is made to General Data Protection Regulations. Whilst this appears to be in line with peer funds the council may wish to consider the inclusion of this within all job descriptions where the postholder is required to handle personal data.

4.11. It is important to acknowledge that the recently recruited Head of Pension Administration and Head of Pension Fund welcomed this review and are aware of the need to strengthen the documents provided to data subjects. An additional recruitment exercise has recently been completed for the post of Pensions Manager – Governance and Compliance and this this officer has been delegated with responsibility to lead on this area.

5. Action Summary

5.1. The table below summarises the actions that have been agreed together with the risk:

Risk	Definition	No	Ref
High	This is a major control weakness requiring attention.	2	2 & 3
Medium	Existing procedures have a negative impact on internal control or the efficient use of resources.	1	1
Low	This represents good practice, implementation is not fundamental to internal control.	1	4
	Total number of agreed actions	**4**	

5.2. Full details of the audit findings and agreed actions are contained in the detailed findings section below.

5.3. As part of our quarterly progress reports to Audit Committee we track and report progress made in implementing all high priority actions agreed. Medium and low priority actions will be monitored and re-assessed by Internal Audit at the next audit review or through random sample checks.

6. Acknowledgement

6.1. We would like to thank all staff that provided assistance during the course of this audit.

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
1	**GDPR Training** We were informed during the audit that there had been a recent report of a personal data breach within pensions administration. Whilst a thorough investigation was undertaken by the Head of Pensions Administration with remedial action taken and appropriate safeguards put in place for the future, we note that there was a missed opportunity to recognise the issue as a data breach by the Pensions Officer initially responsible for handling the affected scheme member's enquiries. In this case this delay did not result in any further breach of personal data. However, failure to act in a timely manner could result in further breaches of data and also risk the council's ability to report, if required, to the Information Commissioners Officer within statutory timeframes. We understand there have been no further reports of suspected personal data	Failure to identify suspected personal data breaches could result in further data loss and result in reputational damage and financial penalty to the council and the fund and cause harm/distress to affected individuals.	Medium	All staff are regularly required to complete the Information Governance training module – it was a compulsory task for staff when they TUPE transferred on 1/12/20 and for all new starters since. Completion and a test pass email will go straight to ICT. Shortly after the data breach staff were reminded that any such incidents should be escalated to their Manager asap and that there is an online form and process on the intranet.

Ref	Finding	Potential Risk Implication	Risk	Agreed Action	
	breaches relating to the pensions service within the current financial year.				
Responsible Officer:		Paul Punter	**Target Implementation Date:**		Complete

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
2	**Privacy Notices** Under the General Data Protection Regulations (GDPR) any organisation that processes personal data is required to inform the data subject of what information is held, how this is collected, retained and utilised. This is commonly achieved through the issuing of Privacy Notices. The Local Government Association (LGA) commissioned a legal firm to create template 'summary' and 'full' Privacy Notices which would be made available to LGPS funds to adapt and adopt. These templates are available via the Local Government Pension Scheme (LGPS) website and are dated May 2018. The summary version is intended to be a simpler guide with the full version containing more detail. The LGA expects both versions to be available to data subjects. The full template Privacy Notice states that *"This template will need to be tailored to the specific circumstances of each fund."*	The current full Privacy Notice is not compliant with the requirements under the General Data Protection Regulations to act in a transparent manner and provide the "identity" of data controllers. Whilst this information may be available upon request this, in addition to the lack of a summary Privacy Notice, is not in line with the expectations under GDPRs relating to ease of access.	High	The Fund will develop a new 'full' Privacy Notice and design a 'summary' Privacy Notice. In doing so regard will be had to the need to refer to Internal Audit and the additional information needed, as identified in this report.

Ref	Finding	Potential Risk Implication	Risk	Agreed Action	
	We understand that a summary Privacy Notice has not been made available to scheme members. Whilst the full Privacy Notice is available to Members via the East Sussex Pension Fund website, we found that it is incomplete. For example, the table contained within the *"organisations that we may share your personal data with"* does not identify the "identity" of the data controllers as required under Article 13 of the GDPRs and detailed in the template document. We also found that that the table does not include reference to Internal Audit nor companies such as those providing data cleansing support which have recently been engaged by the council.				
Responsible Officer:		Michael Burton	**Target Implementation Date:**		31 July 2021

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
3	**Data Retention** Under the General Data Protection Regulations data subjects have a right to be informed of the length of time their data will be held for. The full Privacy Notice includes a statement on *"how long we keep your data"* and states that data will be held for as long as needed to fulfil the duties of the pension fund. This expands to state " *In practice, this means that your personal data will be retained for such period as you (or any beneficiary who receives benefits after your death) are entitled to benefits from the Fund and for a period of 15 years after those benefits stop being paid."* However, the Data Protection Impact Assessment, drafted as part of the project to return the pensions administration service to sovereign control, states that *"Data is stored for the lifetime of the Scheme."* The LGPS template includes footnotes recognising the difficulty of pension funds	The information given to data subjects via the Privacy Notice regarding the retention of their data is incorrect and not in line with current practice. This is therefore not compliant with the requirements under the GDPRs and risks reputational damage to both the council and the fund. In addition to this there is a risk of financial loss due to fines being imposed by the Information Commissioner's Office. The lack of inclusion of scheme member data within the corporate Records Retention and Disposal Policy may lead to a lack of oversight and scrutiny of the treatment of such data.	High	It is noted and agreed that there is a disparity between the existing Privacy Notice and the length of time data is held. The Privacy Notice is to be re-considered, see recommendation 2 (above). Since the Privacy Statement was drafted claims against other schemes have shown that deleting data so soon after a benefit stops being payable can lead to findings of fault as the position cannot be adequately defended. For example, a member who transfers out aged 30 could raise a claim stating they are still a member and entitled to a payment at age 60 and we would not have the evidence to disprove this. The LGA has suggested different retention dates for different elements of data, whilst it acknowledges the difficulty in being GDPR compliant and that the risk of sanction is low. We will

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
	to comply with GDPRs in relation to the retention of member data due to the nature of pension schemes. This template states that holding data indefinitely is *"unlikely to comply with GDPR"* and advises that there may be certain categories of data that could be removed from scheme records at earlier dates. The council has a corporate Records Retention and Disposal Schedule which includes reference to Pension Administration but not the treatment of scheme member data.			take these into account as part of our consideration of next steps. A new policy will need to be approved by the Pensions Board & Committee before being formally adopted.
Responsible Officer:		Michael Burton	**Target Implementation Date:**	30 September 2021

Ref	Finding	Potential Risk Implication	Risk	Agreed Action
4	**Job Descriptions** The service is currently in the process of recruiting to a number of vacancies following the return of Pensions Administration to sovereign control. A review of four job descriptions for posts that were advertised at the time of the audit identified that: • reference to the Local Government Pension Scheme (LGPS) regulations and qualifications/experience were included where relevant. • none of the four job descriptions contained reference to General Data Protection Regulations (GDPR), information governance or data security. Benchmarking of pensions related roles advertised by other public sector bodies identified that: • 50% contained reference to the scheme regulations e.g. LGPS. • 25% contained reference to GDPR.	Newly recruited employees, or those (TUPE) transferring, may lack awareness regarding their specific responsibilities under GDPR and in relation to data security. This may lead to the mishandling of data or non-identification of data breaches and result in reputational damage and financial penalty to the council and the fund and cause harm/distress to affected individuals.	Low	A review will be undertaken of job descriptions for posts within the Pension Fund. Where appropriate a knowledge of GDPR will be added either as essential or desired knowledge. Upon appointment all staff are tasked with undertaking training on data security. Staff cannot access external websites etc until this training is complete, this training is refreshed annually. When the Training Co-ordinator is in post a review will be conducted of further available training on this topic to boost officer understanding of data security. This training will also be provided to Local Pension Board and Pension Committee members as appropriate.

Ref	Finding	Potential Risk Implication	Risk	Agreed Action	
	Whilst it appears that the job descriptions are broadly in line with those of peer organisations, best practice would be for the expectations in relation to GDPR responsibilities to be defined.				
Responsible Officer:		Michael Burton	**Target Implementation Date:**		30 September 2021

Appendix A

Audit Opinions and Definitions

Opinion	Definition
Substantial Assurance	Controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Reasonable Assurance	Most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Partial Assurance	There are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk.
Minimal Assurance	Controls are generally weak or non-existent, leaving the system open to the risk of significant error or fraud. There is a high risk to the ability of the system/service to meet its objectives.

Management Responsibilities

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

This report, and our work, should not be taken as a substitute for management's responsibilities for the application of sound business practices. We emphasise that it is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.