Appendix 1

Internal Audit Report 2018/19

St.Helens Council

Merseyside Recycling and Waste Authority
General Data Protection Regulations

Contents

Assignment Control

	Date
Draft Report Issued	15/11/18
Management Responses Received	04/12/18
Senior Management Approval	10/12/18
Final Report Issued	10/12/18

Distribution

For Action:

Paula Pocock	Assistant Director - Business Services and Strategy
Colette Gill	Marketing and Communications Officer / Data Protection Officer
Nicola Hodge	Data and Performance Manager
Jane Nolan	Business Services Manager

For information:

Carl Beer	Chief Executive
Peter Williams	Director of Finance

Ref:	**MRWA18**
Status:	**FINAL**
Date Published	**10/12/18**

Report Prepared by:

Nicola Colquitt	Senior Auditor
Andrew Paton	Senior Information Management Officer
Barbara Aspinall	Audit Manager

AUDIT & ASSURANCE

COMPLIANCE WITH THE PUBLIC SECTOR INTERNAL AUDIT STANDARDS NWCAE GROUP FEBRUARY 2018

St.Helens Council

Merseyside Recycling and Waste Authority

General Data Protection Regulations

1.1 Introduction

An audit review of compliance with the General Data Protection Regulations (GDPR) was undertaken as part of the 2018/19 Internal Audit Plan. The purpose of the Audit was to provide an assessment of the adequacy of the control environment established, to ensure that objectives are achieved and risks are adequately managed.

1.2 Scope

The review considered policies and procedures, internal processes and systems and information sharing with third parties.

1.3 Background

Context

The Data Protection Act (DPA) 2018, which encompasses the General Data Protection Regulations (GDPR), places a legal obligation on all organisations to process personal data in accordance with appropriate safeguards and to ensure adherence to the six data protection principles, the data controller principle and the rights of data subjects.

The General Data Protection Regulations came into effect on the 25th May 2018, and many previous recommended good practices became mandatory for organisations. It is the responsibility of the Authority's Data Protection Officer to ensure that the Authority complies with these regulations, and must be able to evidence this.

1.4 Audit Opinion

Internal Audit contribute to the overall governance of the Authority by providing an opinion on how effectively risks are being managed and the adequacy and effectiveness of internal control in relation to the areas under review.

Our opinion is based on the work performed as described in the above scope, which was agreed with management prior to the commencement of the review.

Our overall opinion, following this review is as follows:

Substantial Assurance	The majority of expected controls are in place but there is some inconsistency in their application. Whilst there is basically a sound system of controls, there may be weaknesses in the design and/or operation of these and recommendations have been made to enhance the control environment further.

1.5 Agreed Action

Actions to address the recommendations made in this report are included in section 4, which has been agreed with the relevant Managers.

Merseyside Recycling and Waste Authority

General Data Protection Regulations

To gain assurance that the following control objectives are being achieved within an appropriate framework of control:

1. Policies and procedures relating to Data Protection are in place, have been reviewed regularly and are available to all staff.

2. Internal systems and processes are in place and have been revised to comply with the General Data Protection Regulations.

3. Processes for which information is shared with third parties have been appropriately considered and agreements are in place.

Merseyside Recycling and Waste Authority

General Data Protection Regulations

The main findings from our review are highlighted below, and our detailed findings and recommendations are included in Section 4.

3.1 Areas of Good Practice

- Key internal systems and processes have been reviewed and developed to ensure compliance with GDPR.
- An Information Sharing Agreement (ISA) is currently in draft, which is detailed and appropriate to govern the sharing of information with contractors. The ISA is scheduled to be signed by all parties by 30th November 2018.

3.2 Key Areas for Development

There are no areas for development resulting from this audit review.

3.3 Recommendation Summary

In order to assist management in using our reports, we categorise our recommendations according to their level of priority, please see section 5 for definitions.

This table details the number of recommendations made for each level of priority.

Low priority recommendations are provided at the exit meeting, and are not included in this report.

Priority	Number
High	0
Medium	3
Low	2

REF.	FINDINGS	IMPLICATIONS / RISKS	RECOMMENDATION	MANAGEMENT RESPONSE
Control Objective 1: Policies and procedures relating to Data Protection are in place, are reviewed regularly and are available to all staff.				
1	There is currently no distinct Data Protection Policy in place. Although elements of data protection are covered by the Code of Conduct or the Internet and Email Policy, key areas such as Data Breaches and restricting the removal of personal information from site are not documented.	Staff may not be fully aware of their responsibilities in all aspects of Data Protection.	A Data Protection Policy should be developed which includes all elements of data protection. **Priority: Medium**	**Agreed Action:** Produce more explicit guidance. Decision to be made by Business Services Manager regards separate policy or inclusion in Code of Conduct. **Responsible Officer:** Data Protection Officer / Business Services Manager **Timescale:** 31st March 2019
Control Objective 2: Internal systems and processes are in place and have been revised to comply with the General Data Protection Regulations.				
2	Detailed Privacy Notices are in place for both staff and members of the public. However, there is no detail on how consent can be withdrawn when the basis for processing is consent based.	The Authority may not fully comply with legislation, which could lead to sanctions, including monetary fines.	Detail on how consent for holding personal information can be withdrawn by data subjects should be included in the Privacy Notices. **Priority: Medium**	**Agreed Action:** Amend Privacy Notices to include withdrawal of consent. Implemented November 2018 **Responsible Officer:** Data Protection Officer
3	A draft Retention Schedule is in place, however, it does not contain the retention periods for all of the types of information held.	Documents may be retained for an inappropriate period of time.	Retention periods should be agreed for all types of information held, and the Retention Schedule finalised. **Priority: Medium**	**Agreed Action:** Complete Retention Schedule post a review of Email Retention. **Responsible Officer:** Data Protection Officer **Timescale:** 31st March 2019

Assurance Levels

High Assurance	All expected controls are in place and being applied consistently and effectively and there is a sound system of control designed to ensure the achievement of the service or system's business objectives.
Substantial Assurance	The majority of expected controls are in place but there is some inconsistency in their application. Whilst there is basically a sound system of controls, there may be weaknesses in the design and/or operation of these and recommendations have been made to enhance the control environment further.
Limited Assurance	A number of expected controls do not exist or are not applied consistently or effectively. There are weaknesses in the design or operation of controls that could impact upon achievement of the service or system's business objectives and these may have resulted in the emergence of key issues.
Minimal Assurance	A significant number of expected controls are not in place or there are significant weaknesses in the control system that may put the service or system's business objectives at risk. A number of recommendations have been made and / or key issues identified.

Recommendation Priority

High	Issues that are fundamental to the system of internal control for the area subject to review.
Medium	Issues where improvements in control are required to reduce the risk of loss, error, irregularity or inefficiency.
Low	Issues that merit attention and would improve the overall control environment.