

**INTERNAL AUDIT REPORTS - GENERAL DATA PROTECTION REGULATIONS
AND ENVIRONMENTAL MANAGEMENT SYSTEM
WDA/03/19**

Recommendation

That Members:

1. Note the contents of the reports from the Internal Auditor; and
2. Approve the Authority's response to the Key Issues and recommendations identified by the Auditor in the action plans to their reports (at Appendix 1 and Appendix 2).

THIS PAGE INTENTIONALLY BLANK

**INTERNAL AUDIT REPORTS - GENERAL DATA PROTECTION REGULATIONS
AND ENVIRONMENTAL MANAGEMENT SYSTEM
WDA/03/19**

Report of the Treasurer

1. Purpose of the Report

- 1.1 The Authority is required to maintain an effective Internal Audit as a part of its statutory governance arrangements. The Authority's Internal Audit is provided by St Helens Council. The Auditor reviews the arrangements at the Authority and reports to Members on any weaknesses and recommends improvements. This report brings to Members attentions the outcome of the latest review.

2. Background

- 2.1 The agreed audit plan for the year included a review of the Authority's arrangements for compliance with the General Data Protection Regulations (GDPR) and separately for a review of the Authority's Environmental Management System (EMS).
- 2.2 Internal Audit have completed their reviews and their reports on their findings are attached at Appendix 1 (GDPR) and Appendix 2 (EMS). Their findings are summarised below.

3. General Data Protection Regulations (GDPR)

- 3.1 The review considered the Authority's:
- Policies and procedures
 - Internal processes and systems; and
 - Information sharing with third parties.
- 3.2 The Auditor's detailed report is attached at Appendix 1 to this report.
- 3.3 The Auditor concluded that in their overall opinion substantial assurance could be taken from the system and the way it was operated. This means that:

“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.”

3.4 The Auditor identified two areas of Good Practice; these are:

- Key internal systems and processes have been reviewed and developed to ensure compliance with GDPR; and
- An Information Sharing Agreement (ISA) is currently in draft, which is detailed and appropriate to govern the sharing of information with contractors. The ISA was scheduled to be signed by all parties by 30th November 2018. (This has not been finalised yet as it is complex and both parties are actively reviewing the proposed agreement in detail).

3.5 There were no Key Areas for Improvement.

3.6 The Auditor has made three medium priority recommendations for improvement, these are set out in the detailed findings to their report (attached at Appendix 1) and action has been agreed to ensure they are addressed.

4. Environmental Management System (EMS)

4.1 The review considered the internal monitoring processes in place to ensure compliance with the standard that the Authority has signed up to for EMS which is the ISO 14001:2015.

4.2 The Auditor’s detailed report is at Appendix 2 to this report.

4.3 The Auditor concluded that in their overall opinion substantial assurance could be taken from the system and the way it was operated. This means that:

“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.”

4.4 The auditor identified no areas where a high priority recommendation for improvement was required to be made.

- 4.5 The auditor made three medium priority recommendations for improvement, these are set out in the detailed findings to their report (attached at Appendix 2) and action has been agreed to ensure they are addressed. These findings have been identified by the auditor as key areas for development.

5. Risk Implications

- 5.1 The risks that the Authority did not respond to the requirements of the GDPR and EMS have been assessed by the auditor. Their conclusion is that the Authority's arrangements give substantial assurance, and their recommendations for improvements are agreed and are either implemented or will be implemented as agreed. The remaining risk is considered to be low.

6. HR Implications

- 6.1 There are no new HR implications

7. Environmental Implications

- 7.1 There are no new environmental implications

8. Financial Implications

- 8.1 There are no new financial implications.

9. Legal Implications

- 9.1 The Authority's arrangements give assurance that it will meet the legal requirements of the GDPR regime and the EMS standard.

10. Conclusion

- 10.1 Internal Audit reviewed the arrangements for GDPR and EMS and concluded that 'Substantial Assurance' could be taken from both sets of arrangements.
- 10.2 There were no Key Areas for Improvement for GDPR while those identified for EMS arise from medium priority recommendations. Plans are in place to implement all the medium priority recommended improvements from each report.
- 10.3 Members are asked to note the report and to approve the response to the issues it identifies.

The contact officer for this report is: Peter Williams
7th Floor, Number 1 Mann Island, Liverpool, L3 1BP

Email: peter.williams@merseysidewda.gov.uk

Tel: 0151 255 2542

Fax: 0151 227 1848

The background documents to this report are open to inspection in accordance with Section 100D of The Local Government Act 1972 - Nil.