Juno Women's Aid

Data protection audit report

July 2025

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Following a complaint made to the ICO, Juno Women's Aid (JWA) agreed to a consensual audit and a bespoke paper was created to focus on key areas of JWA's processing. JWA responded positively to the audit process and have demonstrated a proactive approach to improving data protection practices.

The purpose of the audit is to provide the Information Commissioner and JWA with an independent assurance of the extent to which JWA, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk-based analysis of JWA's processing of personal data. The scope may take into account any data protection issues or risks which are specific to JWA, identified from ICO intelligence or JWA's own concerns, as well as any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of JWA, the nature and extent of JWA's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to JWA.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, remote interviews with selected staff, and a virtual review of evidential documentation.

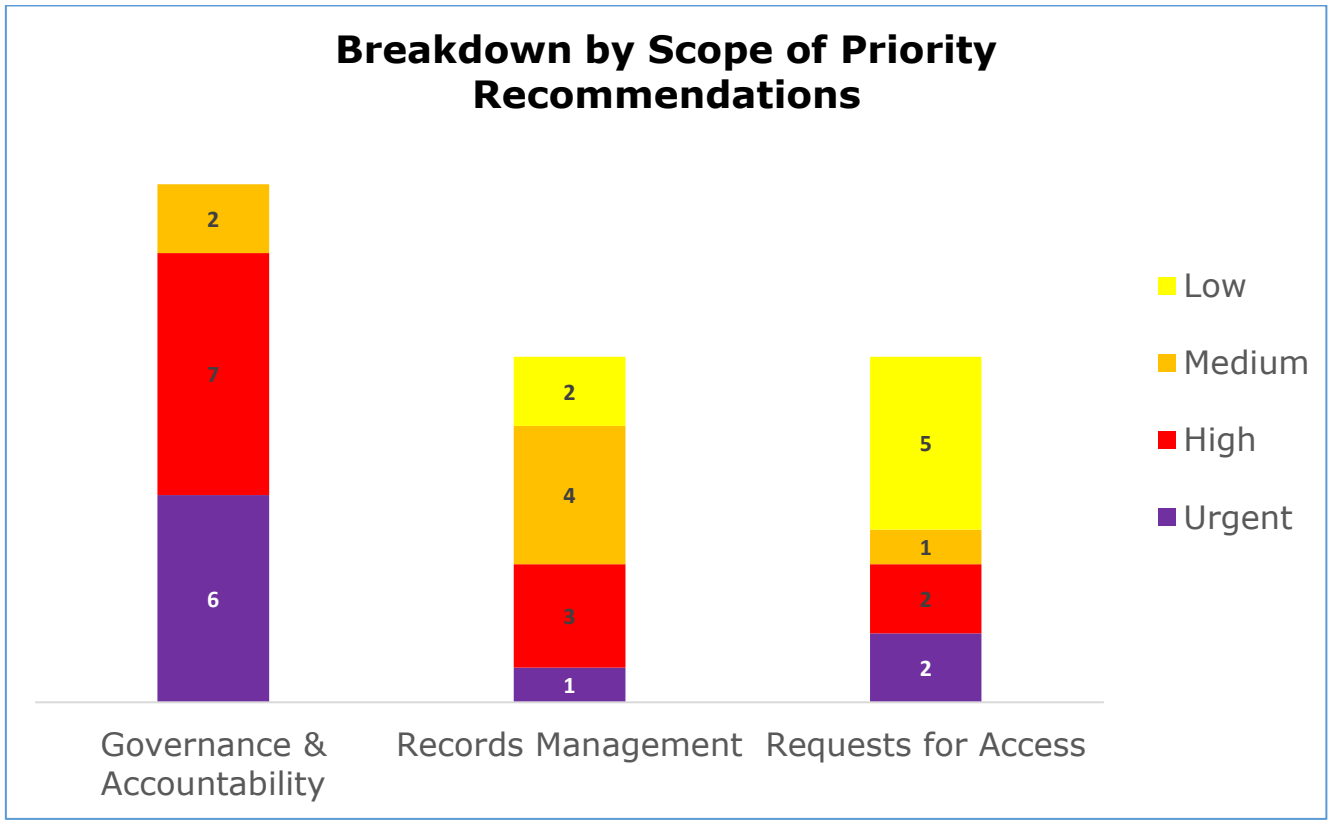
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist JWA in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. JWA's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Requests for Access	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

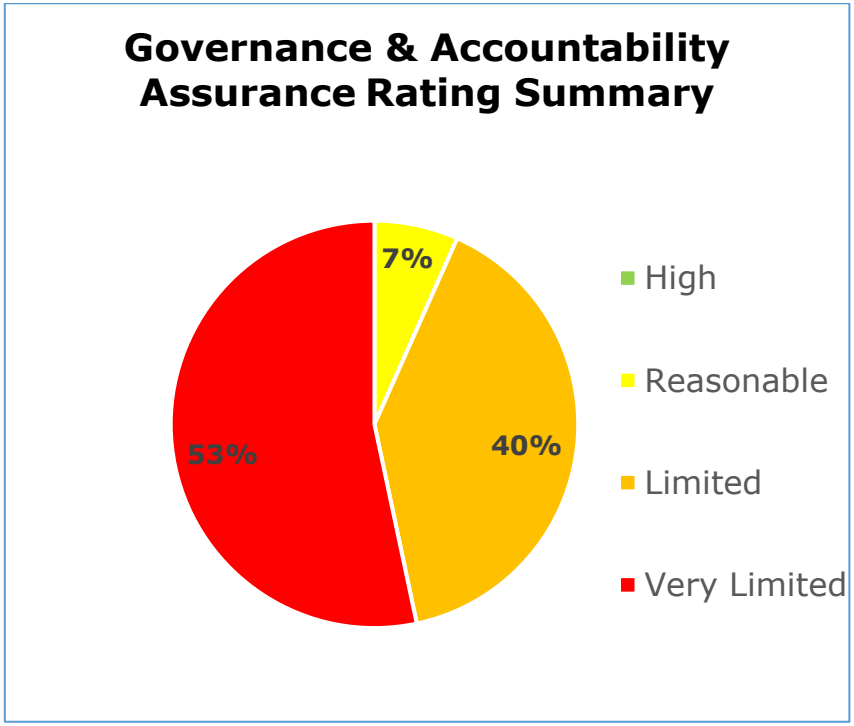
Priority Recommendations



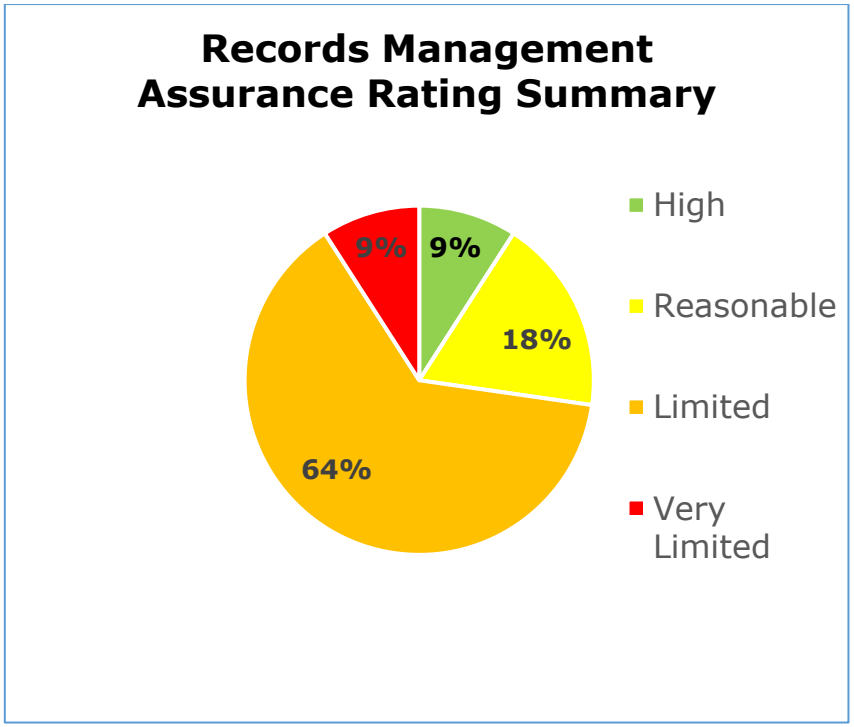
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has six urgent, seven high, two medium and no low priority recommendations.
- Records Management has one urgent, three high, four medium and two low priority recommendations.
- Requests for Access has two urgent, two high, one medium and five low priority recommendations.

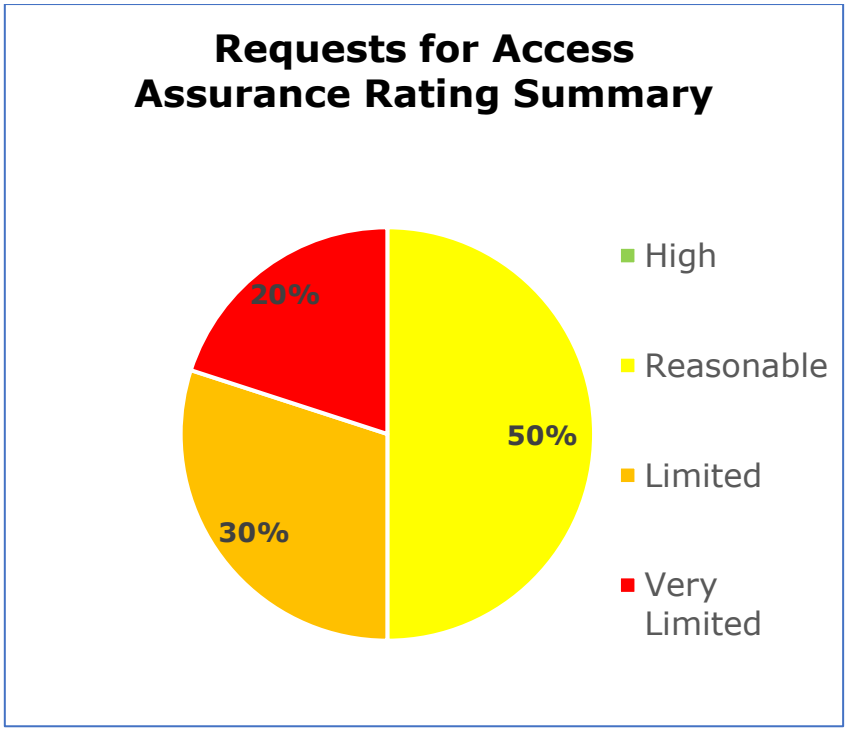
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 7% reasonable assurance, 40% limited assurance, 53% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 9% high assurance, 18% reasonable assurance, 64% limited assurance, 9% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 50% reasonable assurance, 30% limited assurance, 20% very limited assurance.

Key areas for improvement

We identified some key areas within our audit, where JWA needed to implement further measures to comply with data protection law:

Governance & Accountability:

- JWA must review their data mapping exercise to ensure that all processing and sharing activities are documented in the Record of Processing Activities (ROPA). Once the ROPA has been updated, corresponding documentation must be reviewed for consistency including the Appropriate Policy Document (APD).
- JWA must review their use of lawful basis and ensure that the most appropriate basis is selected, documented and conveyed to relevant individuals. JWA must also ensure that privacy information is provided to individuals at the point of personal data being collected.
- JWA must notify individuals of the recent change in lawful basis from the majority use of consent to legitimate interests.
- JWA must complete Data Protection Impact Assessments (DPIAs) for all high-risk processing activities with sufficient detail to demonstrate that JWA have fully considered any impact of that processing to individuals. Where risks have been identified, they should be recorded on a risk register for oversight.

Records Management:

- JWA must review their retention schedule and ensure it captures: all categories of personal data held by the organisation, their respective retention schedules (with consideration of any statutory timescales) and the person responsible for ensuring the schedule is upheld.
- JWA should conduct dip sampling on access rights and include access controls within any planned Data Protection (DP) audits conducted going forward for further oversight of organisational risks.

- JWA should conduct an onsite visit to Radford Archive and Document Storage (RADS), the contracted archiving and confidential waste disposal company, to assure JWA that all personal information is being destroyed in line with contractual obligations. JWA should also ensure that certificates are received from RADs for all personal information that is destroyed on behalf of JWA.

Requests for Access:

- JWA must implement measures to ensure that all requests are passed to the DP lead in good time, which will enable JWA to complete requests within the statutory timescale.
- JWA should include within procedural documentation searches that should be undertaken on all available systems to ensure that all information relating to the individual has been recovered.
- JWA should mark disclosure bundles to determine which copy is retained by JWA and which has been disclosed to the individual.
- JWA must ensure that all complaints, including ones that are reported to the ICO, are logged, monitored and reported to the Board of Trustees for oversight.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Juno Women's Aid.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Juno Women's Aid. The scope areas and controls covered by the audit have been tailored to Juno Women's Aid. and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.