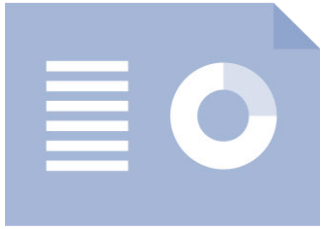
Glasgow City Council

Data protection audit report

December 2024

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.

Glasgow City Council (GCC) were issued with an Assessment Notice on 28 October 2024. This was one of the outcomes of an investigation into GCC's failure to respond to subject access requests (SAR), within statutory timescales. Low response rates had led to a number of complaints being received by the ICO. The Assessment Notice required GCC to participate in a wider audit to establish if there are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data. The purpose of the audit is to provide the Information Commissioner and GCC with an independent assurance of the extent to which GCC is complying with this area of data protection legislation.

The Assessment Notice was carried out between 9-13 December 2024.

The ICO tailored the controls covered in the scope of the Assessment Notice to take into account the organisational structure of GCC and the nature and extent of the GCC's processing of personal data. As such, the scope of this audit is unique to GCC.

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 GCC 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. GCC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Background to the Processing of SARs at GCC

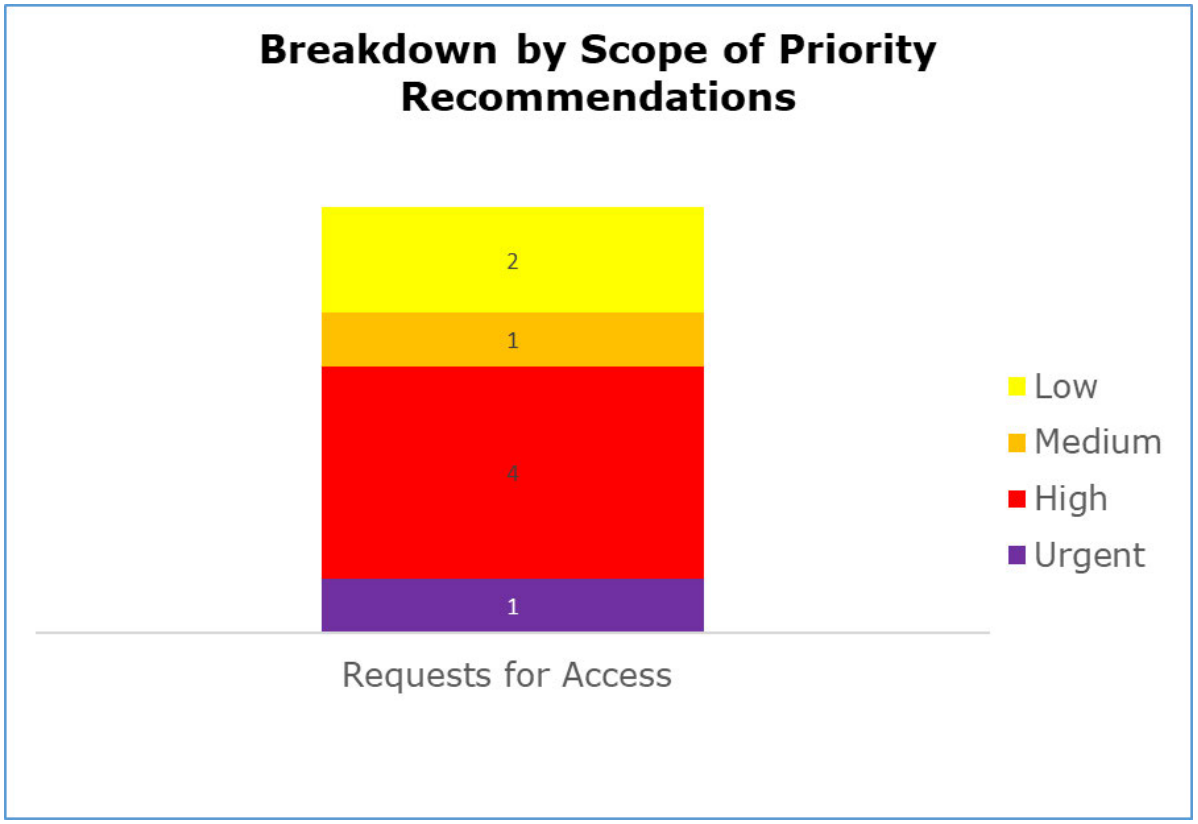
GCC is the local authority for approximately 620,000 people currently. However, the number of people whose personal data is processed will be much greater when including previous residents. In the previous 12 months GCC have received 1368 SARs. These will be managed by one of three areas:

1. Financial Services (FS). SARs are tracked by admin support staff who log requests and direct them to individual services within the FS directorate where the information requested will be held. The service will have responsibility for collating the information and providing a response to the requestor. This area received 54 SARs over the last 12 months and has high rate of responses issued within statutory timescales.

2. The Health and Social Care Partnership (HSCP). The Complaints, FOI and Investigations Team (CFIT) in HSCP are responsible for handling SARs. GCC's current poor response rate and subsequent backlogs of requests that led to the Assessment Notice are confined to this area. It was reported that the issues are primarily due to Scotland's Redress Scheme for survivors of historical child abuse in care in Scotland, which has generated much higher volumes of requests. In addition, a higher proportion of records requested are made up of physical documents which are held in offsite storage. This generated a large backlog during the COVID pandemic when this storage facility was closed for a period of time. Finally, the time needed to collate a response is higher than normal due to the amount of sensitive information contained in these records which requires more careful consideration for exemptions and redactions, as well as additional time to create electronic copies.
   CFIT largely follow the same processes for handling SARs as the other areas although have supplementary procedures to account for the handling of physical records and the nature of the information. CFIT have received 972 SARs over the previous 12 months.

3. Information and Data Protection Team (IDPT). This is a centralised team handing SARs for the Chief Executives' Department, the Neighbourhoods, Regeneration and Sustainability Department (NRS), Education Services as well as requests which relate to the Council as a whole. They also manage SARs on behalf of Glasgow Life however, whilst these follow the same processes they are logged separately and do not form part of GCC's own SAR performance figures. IDPT have received 342 requests over the previous 12 months and have high response rates within statutory timescales.

Priority Recommendations



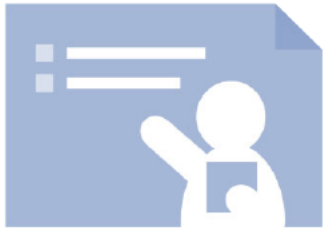
The bar chart above shows a breakdown of the priorities assigned to our recommendations. It contains 1 urgent, 4 high, 1 medium and 2 low priority recommendations.

Areas for Improvement

There is a reasonable level of assurance that processes and procedures are in place and capable of delivering data protection compliance where request volumes fall within available resource limitations. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation. These include:

- GCC should ensure all internal guidance and procedure documents are updated to include current practice and where helpful more detailed processes for certain tasks, for example ID verification, to maintain consistency and resilience in teams that manage SARs.
- GCC should update external facing guidance so that members of the public are informed of all the ways they are able to exercise their right to access their information.
- GCC should ensure that information advising staff about how to recognise SARs and what to do should they receive one is always included in mandatory annual training.
- GCC must take all reasonable steps, including further evaluation of technical and organisational measures, to ensure they are able to meet statutory response timescales.

Audit findings



The tables below identify areas for improvement that were identified in the course of our audit; they include recommendations in relation to how those improvements might be achieved.

Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
The organisation has policies and procedures in place regarding the handling of requests for access	1. GCC's 'Subject Access Request Guide' is available to all staff on the intranet and has recently been updated. The guide includes general information about personal data as well as the legal requirements for responding to SARs. It also includes practical guidance for considering and managing different types or aspects of a request. For example, complex requests, requests from third parties or requests about children. The guide also includes a high level process flow chart including internal timescales that should ensure requests are handled and managed within legislative timeframes. GCC manage SARs using their 'Remedy' system although they recognise that it is not ideally configured to provide full functionality for this purpose. This means that other systems such as an EDRMS and spreadsheets are also used to help manage requests. There are practical reasons why GCC maintain Remedy; however, the incompatibilities mean that staff are also developing their own individual ways of managing certain	GCC should review the methods used by case officers to manage SARs outside the capabilities of Remedy to ensure there are consistent ways of working and casework can be effectively reassigned where necessary. Furthermore, GCC should supplement their 'Subject Access Request Guide' document with these new standardised ways of working for SAR handling teams and consider more detailed procedures for SAR handlers to ensure that expert knowledge and resilience is retained within the organisation following changes in personnel.	High

Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
	aspects of SARs. This means there is a risk of inconsistencies in approach and response developing. In addition, the ability of staff to pick up the full status of casework from other officers, because of absence or leave, can be affected by some information being held on individual outlook account calendars, tasks and reminders, or even physical notebooks. Team members in all SAR handling teams demonstrated consistent ways of working ways of working for most tasks. Knowledge and experience of carrying out these tasks are passed from staff to staff during shadowing and buddy systems of induction and training when new members join the teams. However, the information in the guidance does not match the level of detail, or number of steps, described by staff who carry out this activity. For example, the steps taken to verify identities and capability in requests made for children's information in education settings. This means that much of the expert procedural knowledge is held personally by staff and would leave GCC whenever they left. This creates a risk to the resilience and performance of SAR handling teams following changes in personnel.		
	2. Glasgow City Health and Social Care Partnership's (HSCP) Complaints, FOI and Investigations Team (CFIT) are responsible for the handling of SARs for social care records. The team has its own CFIT Reference Manual document containing similar content and structure to GCC's SAR guide, but it is tailored to specific considerations in processing social care records requests (e.g. the use of exemptions).	GCC should review and update the CFIT reference manual to ensure it continues to reflect the team's current procedures. This means staff will be able to access up to date guidance in line with CFIT's specific practices.	

Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
	The manual's version history identifies an administrative update was made between January 2020 and September 2024 however it has not been subject to a significant update in line with GCC's SAR guide. This means that the manual does not contain up to date information or processes followed by CFIT. For example, the CFIT reference manual does not include their current procedures relating to the use of mandates from solicitors to confirm identities. This means staff seeking guidance on this topic will only have access to the processes detailed in the SAR guide which differ from those used by CFIT.		
Individuals are guided on how to make a request for access (both verbal requests and requests in writing)	GCC have documented guidance on their external facing website that provides information on how to make a SAR. The guidance also includes a SAR privacy statement and a standard request form which can be provided in a paper format where required. The guidance states that requests should be made in writing, with a postal address and email address provided for requests to be sent to. However, no guidance is provided to people who may wish to make SAR verbally. Although GCC may prefer to receive SARs in writing, the legislation does not limit the methods in which people can make a SAR which means verbal requests are valid. In addition, this guidance is not easy to locate on GCC's website. Although the website does contain a search function, members of the public would need to know what to search for in order to find the guidance page. This itself may cause an increase in the number of requests received verbally.	GCC should review the SAR guidance on their external facing website to ensure it is up to date and contains accurate information about making a SAR, including guidance on making verbal requests. Once updated, it should be circulated to staff responsible for handling SARs so that they are aware of the most up to date guidance provided to the public. In addition to this, GCC should ensure the SAR guidance is easily accessible, for instance, including a link in their 'Access to your information' section in their main privacy statement. This will ensure that people are fully informed of their right to request access to their personal data, and how they may exercise it.	High

Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
Staff are made aware of how to identify requests for access (both verbal requests and requests in writing)	GCC have mandatory data protection (DP) training in place that is refreshed on an annual basis. The training content is prioritised and amended every year to ensure it includes current DP areas of change and focus for GCC. For example, this year's training features PCI DSS training about protecting information provided for card payments. However, this prioritisation has meant that the most recent annual training does not include reminders to staff on how to identify requests for access and what to do if they receive one. GCC have developed awareness raising initiatives such as screen savers and intranet blogs to help maintain staff awareness however, these are not mandatory and may not be seen by all staff. If staff do not receive periodic refresher training on how to recognise and channel SARs, their awareness may diminish over time and GCC may fail to meet their legislative responsibilities.	GCC should ensure that their mandatory DP refresher training always includes content reminding staff how to identify a request and what to do if they receive a SAR. This will ensure GCC meet their legislative responsibilities for identifying and responding to SARs.	High
The organisation has processes in place to locate information required in response to a request in good time.	The majority of paper based social care records are held at the Mitchell Library, located in Glasgow City. Glasgow Life, a separate Arm's Length External Organisation (ALEO), has custodianship of these records. Outcomes focused solutions for file location and retrieval have been put in place between GCC and Glasgow Life since the end of the Covid-19 pandemic and the reopening of the library. For example, Subject Access Officers have a base room at the library where retrieved files can be scanned. It was identified during interviews that there are no formalised Service Level Agreements (SLAs) between GCC and Glasgow Life. This risks an inconsistency in process, particularly in the context of high volumes of detailed manual records.	GCC should investigate ways in which service levels could be introduced with Glasgow Life. This would help to improve workstream planning and effective use of resources, particularly in the time pressured task of manual file retrieval for the purposes of fulfilling SARs.	Medium

Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
The organisation properly considers whether or not personal and 3rd party data should be removed	In addition to information within the 'Subject Access Request Guide', GCC have a separate redaction guidance document that staff can refer to for support with redactions. The guidance explains GCC's redaction process and the methods used in order to redact information correctly. However, the guidance was last updated in 2017 and contains some out of date and inaccurate information, such as referring to DPA 1998. In addition, the guidance does not fully reflect GCC's current redaction process as described during interviews. If guidance is out of date and inaccurate, correct procedures may not be followed, particularly following changes in personnel who will not be aware of actual practices. This can lead to inconsistencies in approach and incorrect application of redactions and exemptions which will create a risk of inappropriate disclosure of personal data.	GCC should continue with their plans to review and update their redaction guidance document, ensuring that it refers to the correct legislation (DPA 2018/ UK GDPR) and includes accurate information regarding GCC's current redaction process. Once updated, the newly updated document should be circulated to all relevant staff with responsibilities in the redaction process, such as SAR handlers, paralegals and staff who assist with SARs in services, so that redactions are applied consistently.	Low
The organisation takes a consistent approach in removing personal and 3rd party data from requests	Approval of SAR responses is managed differently depending on the GCC function managing the requests. For example, responses compiled by the information and data protection team (IDPT) are jointly approved by senior case officers within the team and the services the request was made to. This provides assurance that exemptions and redactions are appropriately applied. CFIT does not have a quality assurance process for requests completed by experienced staff members (i.e. to ensure a consistent approach is being taken to exemption and redaction). This creates the risk that different standards are applied. When considering the content of social care records, GCC need to have assurance that exemptions and redactions are applied	GCC should introduce a form of QA or dip sampling of SARs completed by experienced staff in CFIT. This will provide assurance that redactions and exemptions are applied correctly and consistently. This will reduce the risk of harms to requestors or related third parties caused by inappropriate disclosures and support staff in their information rights knowledge and development.	High

Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
	consistently and correctly as inappropriate disclosures could cause significant harms to requestors or related third parties.		
Requestors are given routes of recourse if they are unhappy with the response they have received	Template response letters contained within the 'Subject Access Request Guide' and those used by CFIT along with website SAR form and SAR privacy statement all include detail on how a requestor can complain to the ICO if they are unhappy with a SAR response. Although they all include the correct ICO number; 0303 123 1113, they also include a number that is not valid anymore; 01625 545 745. This risks GCC failing their responsibility to transparency.	GCC should review and update all their guidance and accompanying documents to ensure that they include accurate ICO contact details, so that people are given all necessary information to make a complaint to the ICO where required.	Low
The organisation meets the statutory timeframe when responding to requests	IDPT and Financial Services are able to manage the majority of their SARs within statutory timescales. Where they may not meet 100% these will be the result of specific circumstances to individual requests, rather than ineffective systems or patterns of failure. SARs for health and social care information have been consistently underperforming as a result of high request volumes. These high volumes are reported to be due to Scotland Redress Scheme which offers redress payments to people who were abused while in care as children before December 1, 2004. When the scheme opened, guidance instructed people to submit a SAR request for their files to their local authority in the first instance. This created high volumes of requests, including from people who were ineligible for the scheme. Other factors affecting GCC's ability to respond to requests in statutory timescales include: • Retrieving physical records from offsite storage,	GCC have a statutory responsibility to respond to all SAR requests within one calendar month and must implement all reasonable technical and organisational measures that would ensure they can meet their obligations.	Urgent

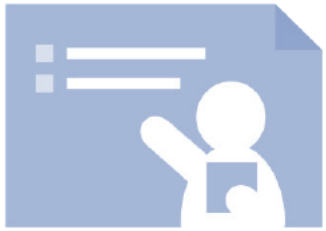
Requests for Access			
Control	**Non-conformity**	**Recommendation**	**Priority**
	• Extended time periods to review and redact large files, • Lack of available financial resource to allocate additional full time personnel to assist with managing requests. GCC identified areas of improvement and developed an action plan to try and improve response rates. They have been working through the actions including: • Installing high volume scanners at offsite storage locations to assist in the retrieval of physical records, • Investigating technical solutions to streamline response processes including the use of AI redaction software, • Redeploying staff and allocating funding for overtime payments to allow additional work on backlogs. • Conducting a Lean Six Sigma review of the SAR process to identify further efficiencies. • Liaising with the Redress Scheme to seek alternative approaches to their current guidance for applicants, to tackle the issue at source and reduce the volume of SARs. Current figures show there are 599 open cases. 163 of these are still within the statutory timescale however, 436 cases have now exceeded this limit without a response being provided. In addition, there are a further 349 cases on hold waiting for proof of ID. This brings the potential total number of cases to 948.		

Observations

The tables below list observations made by ICO auditors during the course of the audit along with suggestions to assist the Council with possible changes.

Requests for Access	
Control	**Observation**
The organisation has policies and procedures in place regarding the handling of requests for access.	1. The ICO would encourage GCC to continue to investigate, where resources allow, alternative or supplementary systems that will improve the efficiency of managing SARs. 2. CFIT maintain a spreadsheet to help manage requests in a system area that does not provide the option for dynamic, multiple editing. This creates some limitations in working (i.e. only one staff member can edit or update at a time). GCC could explore alternative storage solutions that allow collaborative updating of documents (e.g. storing in SharePoint Online).
The organisation has processes in place to ensure that requests are dealt with in a timely manner that meet individual expectations.	Current backlogs from managing high volumes of detailed SARs in CFIT mean that acknowledgement letters are issued to requestors explaining that it is unlikely their request will be responded to within statutory timeframes. Measures have also been put in place to respond to emails from requestors made during the course of the request (i.e. who are following up on how their request is progressing). When backlogs are cleared, or in IDPT or CBS, and where acknowledgement letters do not advise of a delay, best practice would be to keep requestors proactively updated as necessary, particularly where complications in collating information or delays become apparent. GCC could carry out horizon scanning activities to identify potential spikes in request volumes or other risks to SAR management. This would allow GCC to implement measures at the earliest opportunity to mitigate identified risks to their compliance and obligations under Article 15 of the UK GDPR.
The organisation properly considers whether or not personal and 3rd party data should be removed.	GCC could add a link to the redaction guidance document into their 'Subject Access Request Guide' and CIFT SAR guidance documents so that staff are able to access this additional redaction information easily.

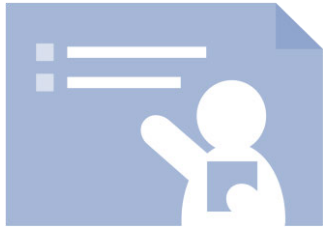
Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits



ICO Audit Team

ICO Engagement Lead – [redacted]
ICO Lead Auditors – [redacted] and [redacted]

Thanks

The ICO would like to thank Dr Kenny Meechan (Head of Information and Data Protection Officer) for their help in the audit engagement.

Distribution List

This report is for the attention of Dr Kenny Meechan (Head of Information and Data Protection Officer).

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 Glasgow City Council.

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 Glasgow City Council. The scope areas and controls covered by the audit have been tailored to Glasgow City Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.