



Senior Information Risk Owner Annual Report

April 2022 - March 2023

May 2023

Contents

Purpose.....	3
1. Overview of key achievements in 2022 - 2023	4
2. Overview of performance related to Information Governance during 2022 - 2023	5
3. Evidence the Councils organisational compliance within the regulatory requirements	6
4. Update on the NHS Data Security and Protection Toolkit (DSPT) and Partnership Working....	7
5. Significant current and emerging Data Privacy, Cybersecurity, and Information Governance (IG) issues.....	7
6. Roadmap of priorities for compliance going forward in 2023 – 2024.....	8
7. Summary.....	9
Appendix A Freedom of Information Act 2000 and EIR requests	10
Appendix B Subject Access Requests (SAR)	14
Appendix C Data Breaches	15

Purpose

The report aims to outline West Lancashire Borough Council's position in terms of our obligation in meeting statutory and regulatory requirements relating to the processing of personal identifiable data under the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA2018) and the Council's duty to be transparent through compliance within the Freedom of Information Act 2000.

It will also aim to provide sufficient information to the Council's Corporate Management Team (CMT) and Cabinet that highlights the work that has been undertaken and the work planned which will continue to strengthen our approach to Information Governance (IG). Whilst continuing to embed a culture across the organisation that is aligned to "Our Data, Our Responsibility" ethos, ensuring that compliance and effective risk management protocols are in place, underpinned by a robust Information Governance infrastructure that is managed and monitored via the Information Governance Committee, who further disseminates information across the Authority to the Service Areas.

Specifically, the report will provide an:

1. Overview of key achievements.
2. Overview of performance related to Information Governance.
3. Information that evidences the Council's organisational compliance within the regulatory requirements relating to the handling of information and provide assurance of ongoing risk management improvement to ensure we meet mandatory standards.
4. Update on the NHS Data Security and Protection Toolkit (NHS DSPT).
5. Detailed overview of the most significant current and emerging Data Privacy, Cybersecurity and Information Governance issues.
6. Overview of the priorities for compliance going forward into 2023 - 2024.

As SIRO, my responsibilities can be summarised as:

- Senior Information Risk Owner (SIRO) for the Council.
- Lead Responsible Officer for fostering a culture that values, protects and uses information for the success of the organisation and benefit of its residents.
- Lead Responsible Officer for maintaining sufficient knowledge and experience of the organisation's business goals with emphasis on the use of and dependency upon internal and external information assets.
- Lead Officer for information risk management in the organisation including resolution of any escalated risk issues raised by the Heads of Service, the Information Governance Manager (DPO) and Information Asset Owners.

The SIRO is supported by the DPO and the Information Governance Officer, who assist the organisation in monitoring internal compliance, informing and advising on information governance obligations, training and also act as a contact point between the Information Commissioner and the Council.

The DPO and the IG Officer also manage the Data Protection and Freedom of Information central records, monitoring performance and compliance with legislation.

Diagram to visualise the SIRO Relationships with officers across the Council



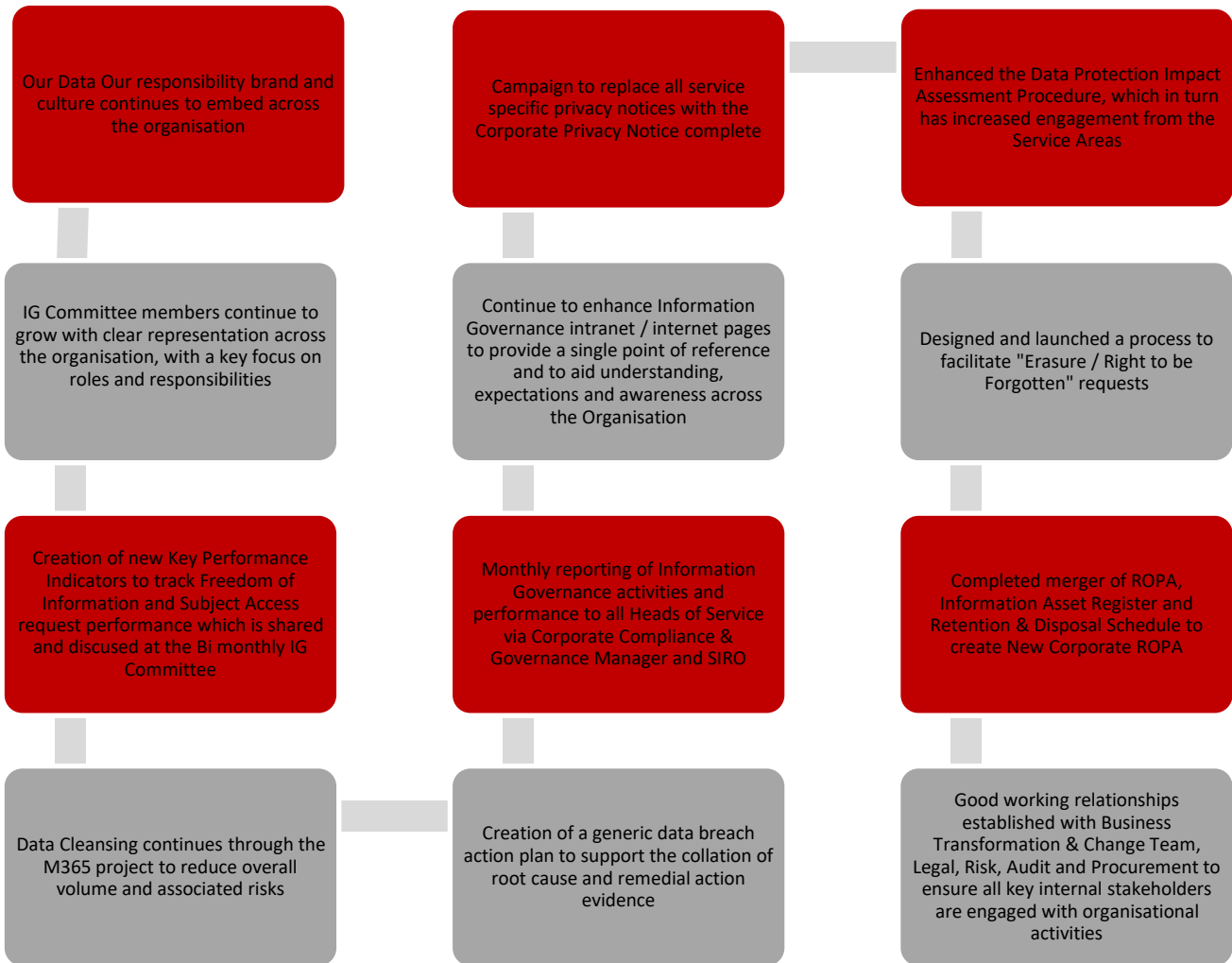
1. Overview of key achievements in 2022 - 2023

It is important to recognise that information is an organisational asset and that a strong information governance culture must continue to be embedded, so that the Council continues to operate lawfully, efficiently and effectively.

Following the significant amount of work undertaken via the Effective Data Management programme and the commitment from officers across the organisation it is pleasing to report that all four Information Governance risks are all currently assessed as cautious.

The risk "Failure to Provide suitable storage arrangements for the Councils electronic information" has been re assessed from comfortable to cautious, due to the further work identified in terms of archiving and retention of data in some legacy systems. This will flow into a piece of work that the Business Transformation and Change team and the ICT Client Manager will facilitate. It is linked to system infrastructure and data management, as part of the digital transformation plan and the formation of the technical design authority.

Key Initiatives Delivered



2. Overview of performance related to Information Governance during 2022 - 2023

- A)** The number of Freedom of Information Act 2000 and EIR requests received for the 22 – 23 period was 637 which represents an increase of 24 (4%) on the previous year. 82% were responded to within the 20-day statutory timescale.
- B)** The number of Subject Access Requests (SAR) made under Data Protection Legislation, which were received by the Council for the period was 673 which represents an increase of 168 (25%) on the previous year, please note the majority of requests were internal. 98% were responded to with the one calendar month timescale.
- C)** The number of Data Breaches for the period was 25 which represents a decrease of 13 (34%) on the previous year. No data breaches were reported to the ICO.

** Please see appendices A, B & C at the end of this report for further detail.

3. Evidence the Councils organisational compliance within the regulatory requirements

Changes to legislation during 2022/2023

There have been no significant changes to primary legislation in the reporting period. We continue to monitor and share where necessary, guidance and developments from our DPO and the ICO.

The Information Governance team are aware of the proposed Procurement Bill which amongst other key objectives will place transparency and integrity at the heart of the procurement system, as such the DPO is engaging with the Procurement Manager to understand the implications on the Council. Our focus will be to ensure that we enhance transparency and remain compliant with Data Protection Legislation.

The DPO is also following the progress of the new Data Protection and Digital Information Bill which is currently progressing through the House of Commons.

Data Protection Impact Assessments

West Lancashire Borough Council manages a variety of information assets which are essential for service delivery. The council has a statutory requirement to ensure that its information systems and supporting processes meet security, confidentiality, data protection and data quality needs. Data protection by design and default is embedded into the Corporate Project methodology with the DPO being recognised as a key stakeholder as scope is defined, which provides assurance that all requirements have been considered for any new or re-configured asset system or business process.

Overall this year there have been 29 DPIA's submitted to the IG Manager for review, challenge and subsequent sign off. This is an increase of 15 on the previous year.

Policies

Existing policies have been reviewed and refreshed. The Data Quality Policy and the Freedom of Information policies have been subject to detailed gap analysis, following which a detailed report and summary of recommendations will be circulated for consideration / implementation.

It is coming up to 12 months since the Pentana Policy module has been in operation providing transparency and a good practice policy management framework. One element is that each policy has an established review date which highlights to policy owners the timescale for review. Already available to all managers a further phase will be to provide access to Pentana to all staff to aid learning and development and further embed understanding and transparency across the Authority.

Reporting

Work has continued during 2022 – 2023 to enhance the reporting of IG performance in a consistent and transparent manner.

4. Update on the NHS Data Security and Protection Toolkit (DSPT) and Partnership Working

During the Covid pandemic arrangements, both legislation and working practices were developed to facilitate the compliant exchange and sharing of personal data, to allow proactive and responsive intervention to emerge, in support of the response and recovery to the emergency.

Recognising the importance of data and insight, when influencing and shaping new service delivery to emerge, it was key that we continued to strengthen this area of work. In partnership with Health, we have co-designed and recruited a joint role (Population Health Intelligence Advisor) between WLBC and the ICB. This role is managed by the Business Transformation and Change Team (WLBC) but works across the organisation and alongside our wider partnership to support the development of data driven interventions that aim to shape thinking and action at a local level to reduce inequalities across West Lancashire.

The Council's DPO continues to work with partners and across the organisation to ensure data sharing agreements are developed / are in place to support the Council's business activities now and in the future.

Data will continue to be a key enabler, therefore, it is important to continue to work with IG leads to strengthen our approach to data, so that when data is used, it is done so, within a compliant framework. This approach, will enable us to deliver the aspirations outlined within our corporate plan, linked to neighbourhood working and reducing inequalities.

Within the pandemic, there was a recognition that access to more partnership data, including a range of NHS patient-related data, allowed a wider view to be taken, linked to people and place. The varied dataset was key in allowing a more insightful view as to what was happening locally at a place and postcode level and how, in collaboration with partners, we could utilise this data to target a range of intervention measures that would reduce risk and support our residents to access services that aim to support their health and wellbeing, whilst reducing inequalities.

To enable this to happen, it is critical that we maintain the highest standards of data privacy for all data shared with the NHS and partners. Following the 2nd successful submission of the NHS Data Security and Protection Toolkit (NHS DSPT), whereby the Council was deemed compliant against the ten data security standards outlined by the National Data Guardian which provides the NHS and other partner organisations with assurance that all personal data is managed securely and in line with legislation. Work is now underway to prepare us for the next submission, which will take place 30th June 2023.

This significant piece of work has been supported by colleagues in Business Transformation and Change team, Audit and our Lancashire County Council Digital colleagues and is a clear example of how we are demonstrating our commitment to continue strengthening our approach to Information Governance.

5. Significant current and emerging Data Privacy, Cybersecurity, and Information Governance (IG) issues

Data Privacy

The significant governance issue that was previously reported has since been closed. There remain two historic audit actions outstanding, with work progressing to mitigate the risk in these areas. The

audit actions will remain open until we are satisfied that there is sufficient robust evidence to allow closure.

Areas for further focus include:

Contracts - Work continues on an all-encompassing contracts workstream to ensure all historic contracts are up to date and compliant with GDPR, Procurement Regulations and NHS toolkit requirements. The contract detail is continually refreshed and represents a robust source of information.

Systems where we have challenges complying with Retention & Disposal – The Council uses a number of legacy systems which due to the age and development architecture are unable to comply with current legislation. The Service areas via the IG Committee have identified a small number of systems where there are challenges complying with Retention and Disposal, this information will flow into the system infrastructure and data management piece of work

Information Security/Cyber Security

Our IT and Cybersecurity services are delivered through a collaboration agreement with Lancashire County Council Digital (LCCD). It is LCCD's responsibility to ensure our councils IT infrastructure has robust policies and procedures in place to help wherever possible prevent attacks against our corporate, employees and customer data. To support this activity WLBC via LCCD engage a third party company to undertake an IT Health Check of the environment. The test took place in February 2023, following which a detailed report will be received and a corresponding action plan will be captured by LCCD to address the gaps identified. This action plan will then support our application for a Public Service Network (PSN) connection compliance certificate later this year.

6. Roadmap of priorities for compliance going forward in 2023 – 2024

Whilst work has commenced on all of the priorities detailed below with 50% having been completed. Looking ahead into 2023 -2025 work will continue in all these areas to strengthen all aspects through the Information Governance and Operational Compliance Mangers Service Action Plan, which will be further supported by the Information Commissionaires Accountability Tracker.





7. Summary

Within the report, strong evidence continues to confirm that the organisation is committed to embedding a robust approach to effective information governance. This continues to be driven by the SIRO, the new DPO, The Information Governance Officer and the Information Governance Committee operating model.

The focus this year will be to continue to strengthen our approach to effective data management, through the introduction of a new operating model, that is committed to creating capacity, capability and continuity, both within the team and across the organisation. This approach will be to strengthen alongside the development of innovative and dynamic processes, housed within effective systems, that evidence improved performance and allow us to target intervention in areas that may require it.

Senior Leaders continue to be committed to embedding a culture of " Our Data, Our Responsibility" as they recognise that the work delivered within the Effective Data Management Project must continue, as this allows us to be a compliant organisation, whilst being efficient and effective in the delivery of the Council's business operating within a transparent decision making framework.

Appendix A Freedom of Information Act 2000 and EIR requests

Emerging themes and planned improvements

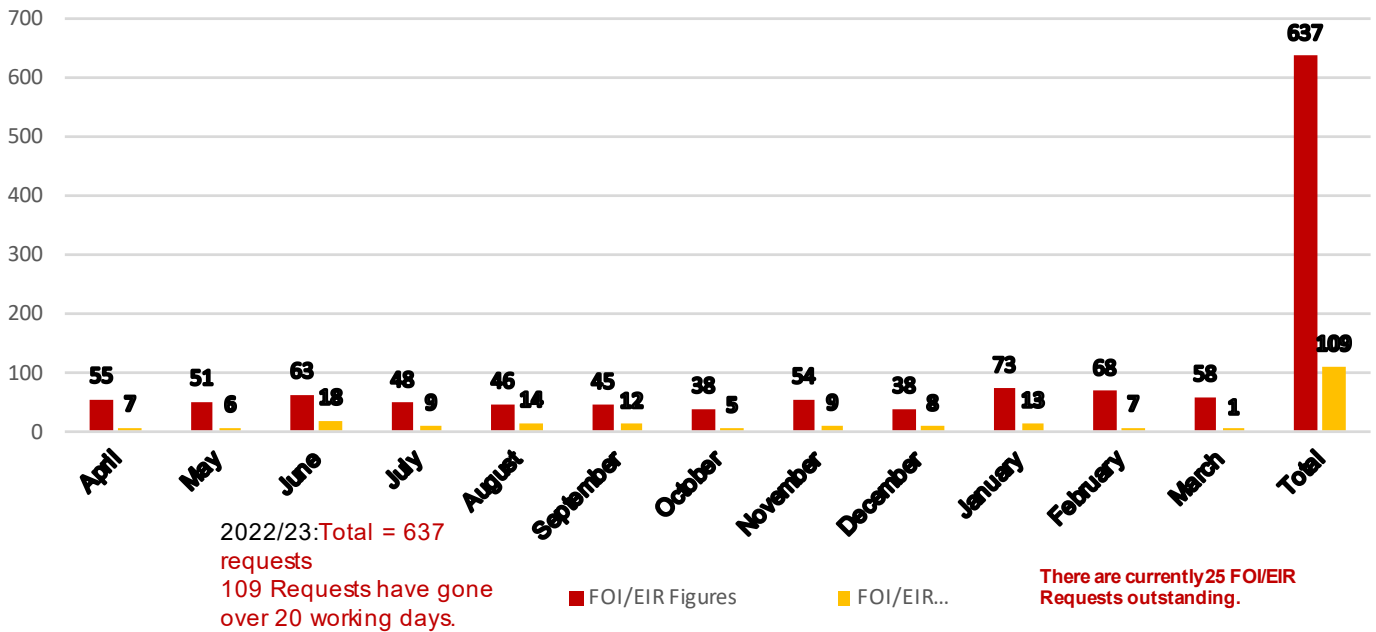
- In terms of the number of requests for an internal review (This is where the requester of the FOI / EIR requests an internal review of the information initially provided), 4 requests were received (versus 10 in the last reporting period). Following the subsequent response, which were all within the 20 day statutory timescale, there were no further escalations made to the ICO, which overall demonstrates the robustness of the evidence supplied.
- It is disappointing to report that we have not been able to deliver a consistent monthly response performance above 90% against the 20 day statutory time limit with an average performance of 82% for the overall 22 – 23 period.
- This has been due to a number of reasons, resource, the turnover of staff and the loss of experience in a few areas, but in particular the number of requests to Planning & Regulatory Service which remains high and constant. Where possible, and for routine enquiries, information is provided on the Council's website to allow the public to view the information themselves. The available staff resources within services remains a challenge, and whilst efforts to support recruitment continue, additional resources have been applied to those services with a higher number of enquiries to help support and coordinate responses during 23/24.
- Remedial action plans were introduced with regular reporting of performance via the IG Committee and to the Heads of Service and the SIRO. As is evident from the February and March data, the actions have been somewhat successful. Monitoring / escalation will continue until a continual upward trend is evident and all areas are reporting positively.

FOI & EIR Requests 2022/23	Number of Requests received	% of responses within 20 working days	Number of requests over 20 working days	Number of internal reviews	Number of complaints to the ICO
Apr	55	87%	7	2	0
May	51	88%	6	0	0
Jun	63	71%	18	0	0
Jul	48	81%	9	0	0
Aug	46	70%	14	0	0
Sep	45	73%	12	0	0
Oct	38	87%	5	0	0
Nov	54	83%	9	1	0
Dec	38	79%	8	0	0
Jan	73	82%	13	1	0
Feb	68	90%	7	0	0
Mar	58	98%	1	0	0
Total	637	82%	109	4	0

FOI/EIR Statistics 2022/23 – Monthly



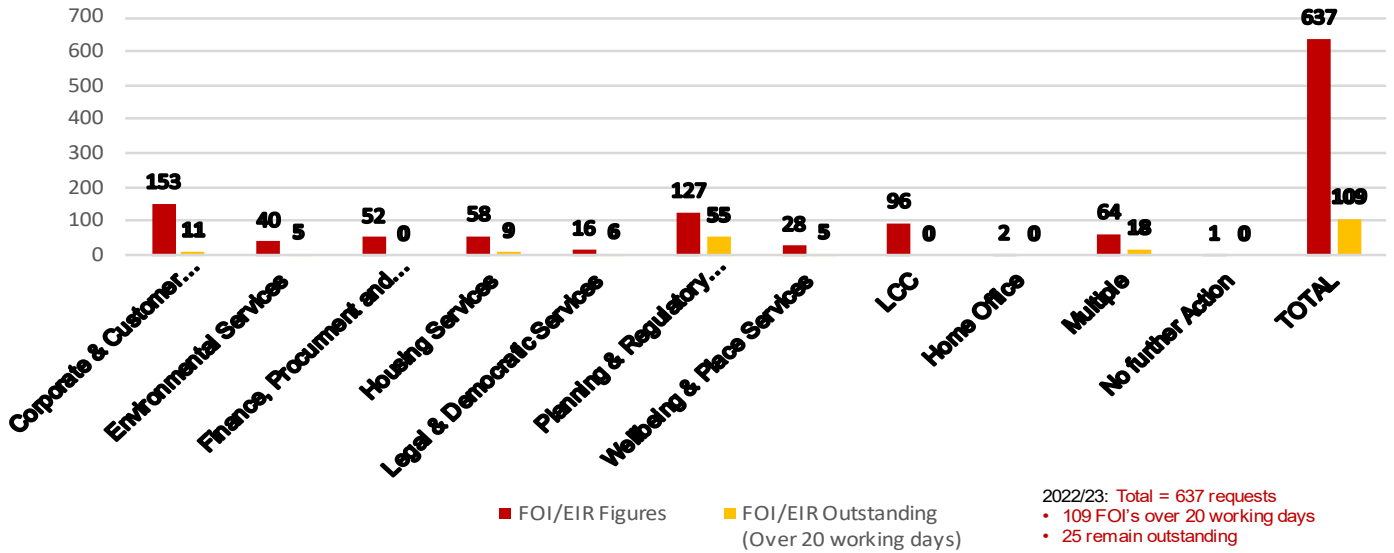
Overall FOI requests from 1 April 2022 – present



FOI/EIR Statistics 2022/23



Overall FOI requests from 1 April 2022 – present



Appendix B Subject Access Requests (SAR)

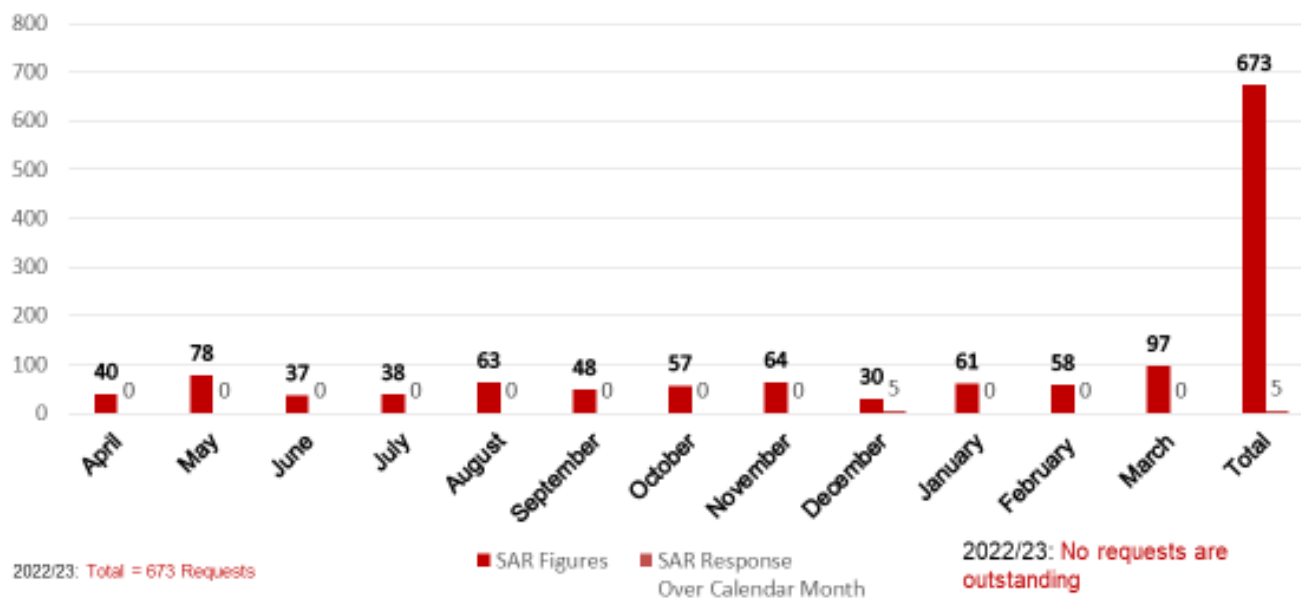
Emerging themes and planned improvements

- 98% of SAR's were responded to within the calendar month statutory timescale with an average response time of 1 to 2 days.
- The increase in overall numbers is a result of the volume of internal requests. All such requests are routed via the DPO and logged to provide a transparent audit trail of requests between service areas, this has provided more robust evidence of demand management.
- Police, statutory body and local authority requests have increased by approximately 5%
- Housing Services have seen an **60%** increase in SARs being raised linked to enforcement protocols

SAR Statistics 2022/23 - Monthly



SAR requests from 1 April 2022 – present



Appendix C Data Breaches

Emerging themes and planned improvements

- Paper / post continues to be highest source linked to breaches
- All breaches were reported within the internal and external timescales of 72 hours.
- All incidents have been fully investigated by the teams with the outcomes shared with the DPO for overview and challenge as to remedial actions undertaken.

The following table shows the number of data breaches and the root cause for the period of 1st April 2022 – 31st March 2023.

Data Breach Statistics 2022/23



Period 1st April 2022 - present

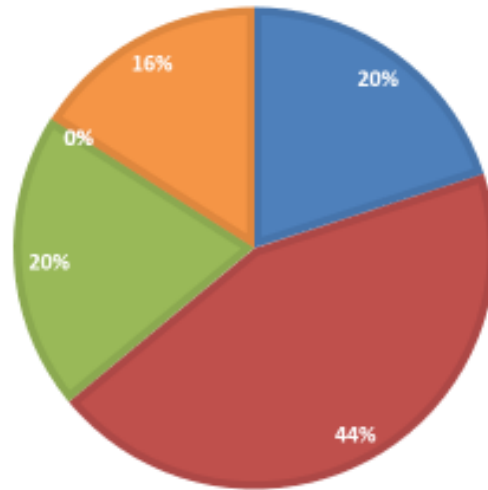


We must celebrate the fact that everyone who has been involved has delivered to the expected standard, hence delivering 100% compliance. 38 Breaches were reported in 2021/22



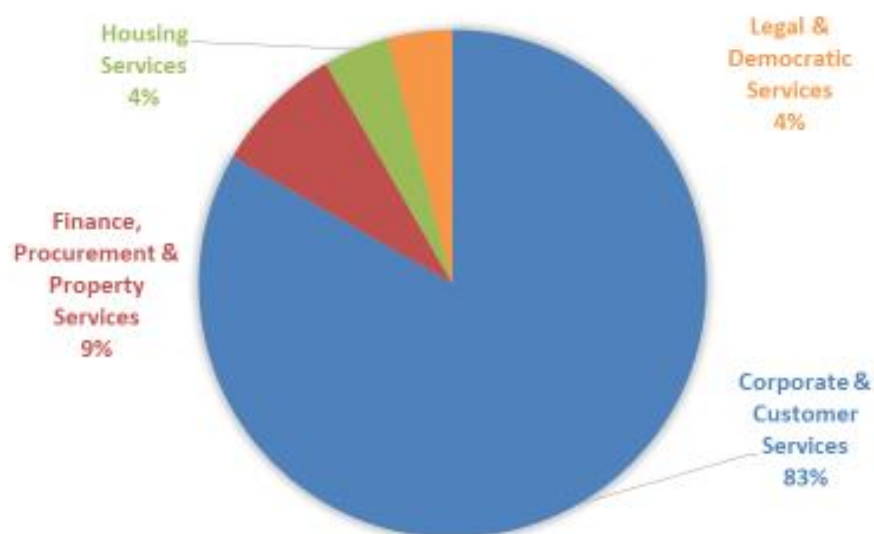
DATA INCIDENTS BY TYPE 2022/23

■ Internal Email ■ External Email ■ Post/Paper ■ Mobile ■ I-Pad ■ Other



The pie chart below represents the volume of data breaches per service area. The highest volume for 22 - 23 was reported by Corporate and Customer Services at 84%. This is a significant increase from the 15% reported in 20 - 21. As a frontline service to the Borough Corporate and Customer Services experience high volumes of interaction from residents, either by face to face, telephone, post or email in comparison to other service areas.

Incidents by Directorate 2022/23



Learning continues to take place, which includes the development and implementation of tools and measures which aim to improve our overall information governance and cyber-security compliance.

The Information Governance Officer and DPO have worked across the Council to create a supportive culture around incident management, to ensure colleagues are not afraid to report incidents, and this is again reflected in the figures we see reported this year.

We have introduced training, robust reporting and empowered staff across the Council to be proactive when a breach occurs, so that we can deal with the issue, but also learn from it.

Colleagues are encouraged to share their concerns and seek advice at any point within the data breach journey.

Cyber Security is not just LCCD's responsibility, good recovery is about senior managers using their knowledge of their information and systems and working with our ICT Client Manager and Information Governance team to be as well prepared as is realistically possible.

Our Information Governance team has collaborated with other teams on a broad range of projects and programmes across the Council, working to ensure that information security, data privacy and regulatory compliance is maintained as new and more efficient ways of working are introduced.

This has included:

- Working with the procurement and the legal team on a new approach to the tendering process, which will include DPIA being part of the procurement checklist moving forward.
- Engagement of the ICT Client Manager to provide advice on Information Governance issues and risks before new assets are purchased.
- Working with colleagues and the programme leads to ensure that information security and cyber security controls are considered in the early stages of a project, in line with Data Protection by Design and Default and ICO expectations.

Whilst this approach has ensured proper mitigation and management of Information Governance risks on many projects, it has also led to an increase in demand on IG resources, which is being monitored, so that we can ensure that resources are being utilised effectively to deliver the desired outcomes.