SENIOR INFORMATION RISK OWNER ANNUAL REPORT

APRIL 2021 – March 2022

Purpose

The report aims to outline West Lancashire Borough Councils position in terms of our obligation in meeting statutory regulatory requirements relating to the processing of personal, confidential or identifiable data under the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 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.

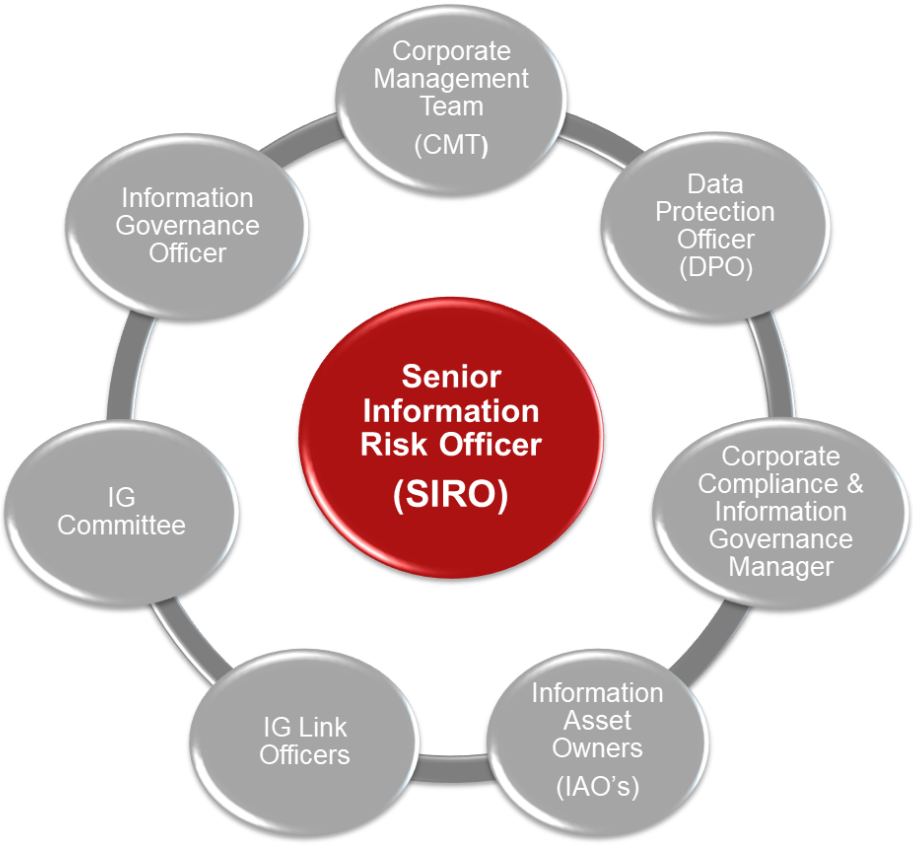
Specifically, the report will provide an:

1. Overview of key achievements.
2. Overview of performance related to Information Governance.
3. Information that evidences the Councils 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 in 2022 - 2023.

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 Data Protection Officer and Information Asset Owners.

Below is a diagram that visualises the SIRO Relationships with officers across the Council



1. **Overview of key achievements in 2021 - 2022**

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.

A key enabler to the work described in this report, has been the successful implementation of the "Effective Data Management project" which has delivered 134 improvements alongside the closure of 45 audit recommendations. These actions are evidenced based and can be accessed at any time. The approach taken has been one of collaboration and connectivity, with strategic buy in, alongside a project sponsor, supported by the Business Transformation and Change Team (previously BID) who, in partnership with key stakeholders enabled the delivery of a robust plan that executed the outlined strategic plan.

Following the significant work undertaken and the commitment from officers across the organisation involved in the Effective Data Management programme of work, it is pleasing to report that during 2021 – 2022 all five IG risks recorded on the Risk Management system Pentana have all been reassessed as either comfortable or cautious.

Key Initiatives Delivered

2. Overview of performance related to Information Governance during 2021 - 2022

A) The number of Freedom of Information Act 2000 and EIR requests received for the period was 613. For the year 20 - 21 there were 662 requests which represents a decrease of 49 (7%). 98% were responded to within the 20 day statutory timescale.

B) The number of Subject Access Requests (SAR) made under Data Protection legislation, that were received by the Council for the period was 505. For the year 20 - 21 there were 191 requests which represents an increase of 62%.100% were responded to with the one calendar month timescale.

C) The number of Data Breaches for the period was 38. 2 were reported to the ICO, with no further action taken. For the year 20 – 21 there were 48 breaches reported which represents a decrease of 10 (26%).

** 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 2020/21

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 Data Protection Officer (DPO) and the ICO.

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. With this in mind, the Council has established and embedded a formal mechanism via its Effective Data Management Programme and associated Information Governance policies, which will provide assurance that all the above requirements have been considered for any new or re-configured asset system or business process.

Policies

During 2021 - 2022 existing policies were reviewed and refreshed and new policies, such as Data Quality and Records Management were produced and implemented to support the organisation in understanding roles and responsibilities in dealing with effective data management. In addition a new Pentana policy module has been created which will house all Council policies. This module will actively trigger policy owners to undertake regular timely reviews and in due course will become visible to all staff to aid understanding and transparency across the Authority.

Reporting

Whilst there is a recognition that the Council has lots of data, much work this year has been undertaken to create new reporting mechanisms, that evidence demand management and performance. This insight is now available and is utilised when reporting to the Information Governance Committee, Senior Leaders and Members. The data provided is now within a consistent approach, evidenced based, allowing informed data driven decisions to be made both strategically and operationally.

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 exchange and sharing of personal data in support of the response and recovery to the emergency.

Building further on the good practice that emerged, linked to sharing data and utilising data to shape service delivery we have co-designed and recruited a joint role (Population Health Intelligence Advisor) between WLBC and the CCG. 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 a range of interventions that are data driven and aim to reduce inequalities across West Lancashire.

The Council's Data Protection Officer (DPO) supported by the Business Transformation and Change team continue to work with partners and across the organisation to ensure data sharing agreements were developed / are in place to support the Council's business activities now and in the future.

This approach has been further strengthened by the successful submission of the National Health Service Data Security and Protection Toolkit (NHS DSPT) in June 2021, whereby we, as an organisation were 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.

As we continue to strengthen our partnership working, and to support us to deliver the aspirations outlined within our Corporate plan, linked to neighbourhood working and reducing inequalities, it is key that any data sharing is done within a compliant framework.

During the Covid pandemic, there was a recognition that we had access to more partnership data, including a range of NHS patient-related data. This varied data allowed us to gain a more insightful view as to what was happening locally at a place and postcode level and how, we as an organisation, in collaboration with partners, could target a range of intervention measures that would reduce risk and support our residents to access services that aimed 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 1st successful submission of the NHS Data Security and Protection Toolkit (NHS DSPT), work is now underway to prepare us for the next submission, which will take place 30th June 2022.

This is a significant piece of work which requires support from the Business Transformation and Change team, Audit and our Lancashire County Council Digital colleagues and is a clear example of how we as an organisation, are demonstrating our commitment to continuing to strengthen our approach to Information Governance.

5. The most significant current and emerging Data Privacy, Cybersecurity and Information Governance (IG) issues

Data Privacy

There are just 2 historic audit actions outstanding that relate to the previous significant governance issue and work is ongoing to mitigate risk in these areas so that they can be concluded.

Areas for further focus include:

Contracts - Work has commence 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 aspiration is to have one "golden source" of contract information that is continually refreshed.

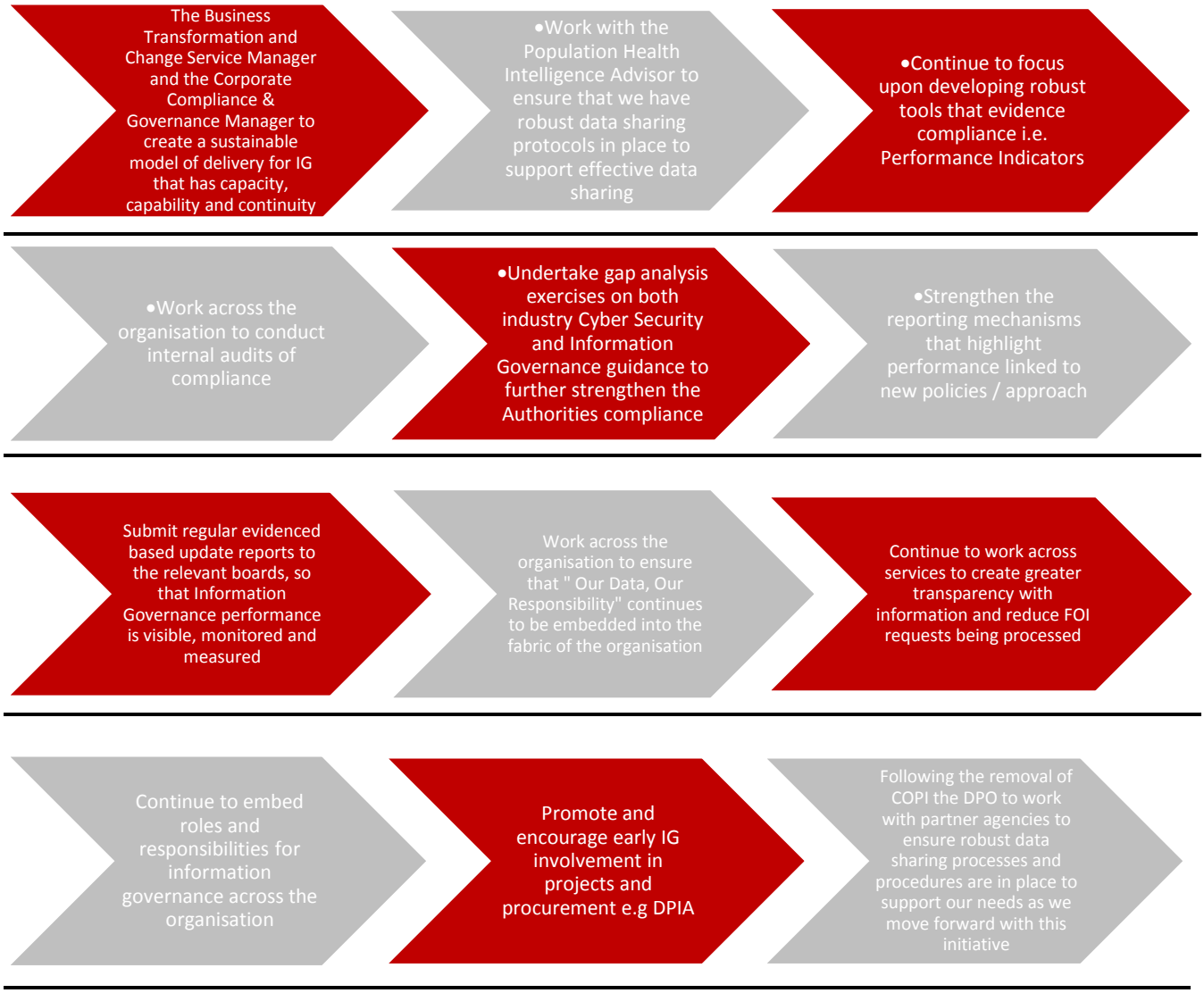
Systems where we have challenges complying with Retention & Disposal – The Council uses a number of legacy systems which, due to the age and development architecture are unable to comply with current legislation. This will flow into a piece of work that the Business Transformation and Change team will facilitate. It is linked to system infrastructure and data management, as part of the development of a digital transformation plan, which will be supported by LCCD.

Information Security/Cyber Security

The perception and understanding of Information Security or Cyber Security has changed considerably over the last two years, with organisations like the National Cyber Security Centre (NCSC) and the Department of Levelling Up, Housing and Communities (DLUHC) leading the way with guidance, training and action plans aimed specifically at organisations such as our Council.

Our IT and Cybersecurity services have been outsourced to Lancashire County Council Digital (LCCD) which was previously managed by BT Lancashire Services (BTLS). 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 data or employees and customers. 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 2022, following which a detailed report has been received and a corresponding action plan has been 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 2022 – 2023



Summary

Within the report, there is strong evidence that confirms that the organisation is committed to continuing to embed a robust approach to effective information governance. This will be driven by the new Information Governance Manager within 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 creates capacity, capability and continuity, alongside the development of innovative and dynamic systems and processes, 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 over the duration of the Effective Data Management Project needs to continue, as this allows us to be a compliant organisation, which supports the efficient and effective delivery of the Council's business in an open and transparent decision making framework.

Appendix A Freedom of Information Act 2000 and EIR requests

Emerging themes and planned improvements

- The introduction of the Revenues and Benefits team to the Corporate and Customer Services area has had an impact on the overall number of requests received.

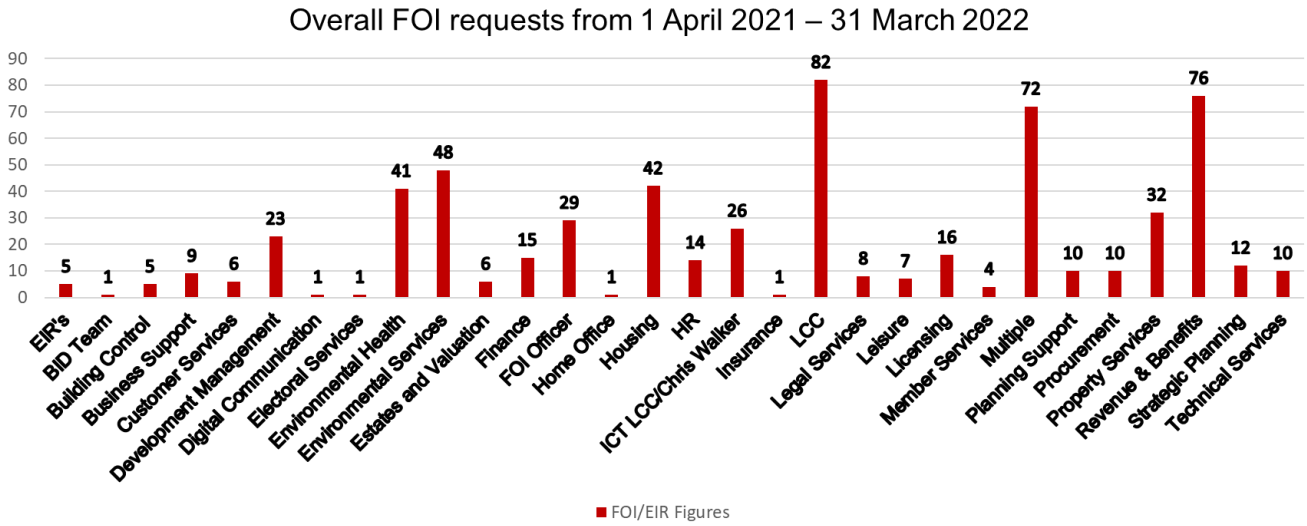
- Increases in topics linked to Lancashire County Council, Housing Stock and Business Grants have led to an approximate increase of 2% on 20 – 21 figures

- 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), requests were up 2% on 20 – 21 with 10 requests received (versus 6 in the last reporting period). Following the subsequent response, which were all within the 20 day statutory timescale, there were no escalations made to the ICO, which demonstrates the robustness of the evidence supplied.

- Data highlights that WLBC have consistently delivered a monthly response performance above 90% against the 20 day statutory time limit with 98% performance for the overall 21 – 22 period.

- Work has commenced to agree a FOI / EIR internal performance indicator which will be in place by the end of September 2022

FOI & EIR Requests 2021/22	Number of Requests received	% of responses within 20 working days	Number of requests where information was granted	Number of requests where information was refused	Number of internal reviews	Number of complaints to the ICO
Apr	48	92%	39	9	1	0
May	59	96%	49	10	1	0
Jun	40	100%	31	9	2	0
Jul	38	99%	31	7	1	0
Aug	59	97%	46	13	1	0
Sep	58	98%	45	13	1	0
Oct	48	99%	34	14	1	0
Nov	52	99%	32	20	0	0
Dec	32	99%	22	10	0	0
Jan	60	100%	39	21	0	0
Feb	65	99%	47	18	1	0
Mar	54	99%	35	19	1	1
Total	**613**	**98%**	**450**	**163**	**10**	**1**



Appendix B Subject Access Requests (SAR)

Emerging themes and planned improvements

- 100% of SAR's were responded to within the calendar month statutory timescale with an average response time of 1 to 2 days.

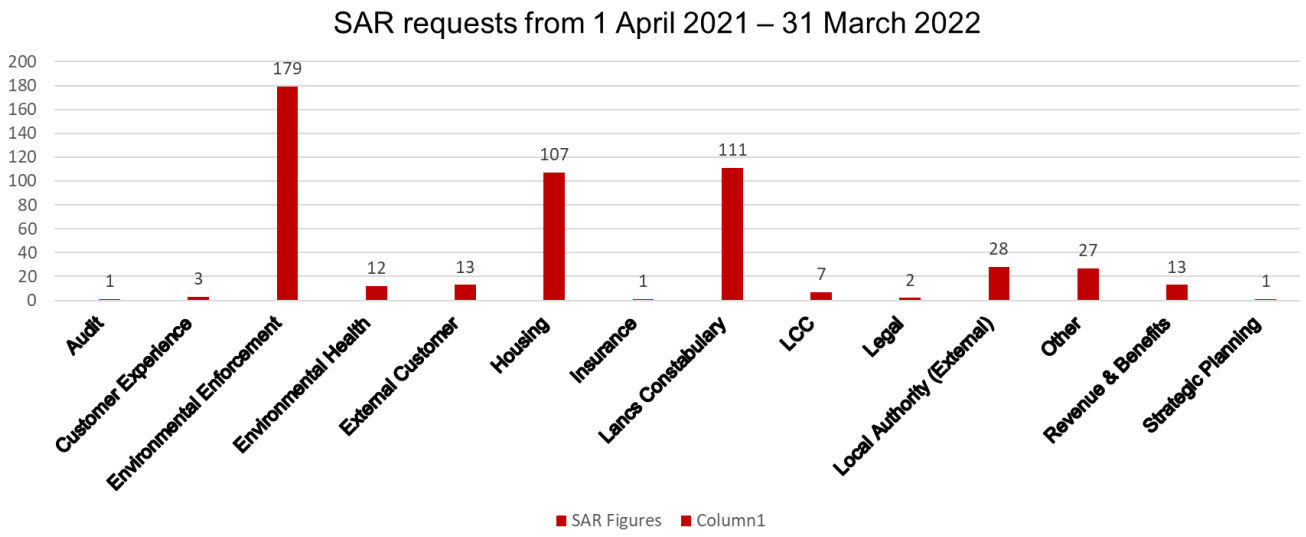
- The number SAR's received by the Council for the period was 505. For the year 20 - 21 there were 191 requests which represents an increase of 62%.

- The increase in overall numbers is a result of an internal SAR logging procedure that has been introduced across the Council, which has provided a transparent audit trail of requests between service areas and has provided more robust evidence of demand management.

- Police requests have also increased by roughly 5%, and other lawful requests by other local authorities.

- Housing Services have seen an **60%** increase linked to enforcement protocols

- Work has commenced to agree a SAR internal performance indicator which will be place by the end of September 2022

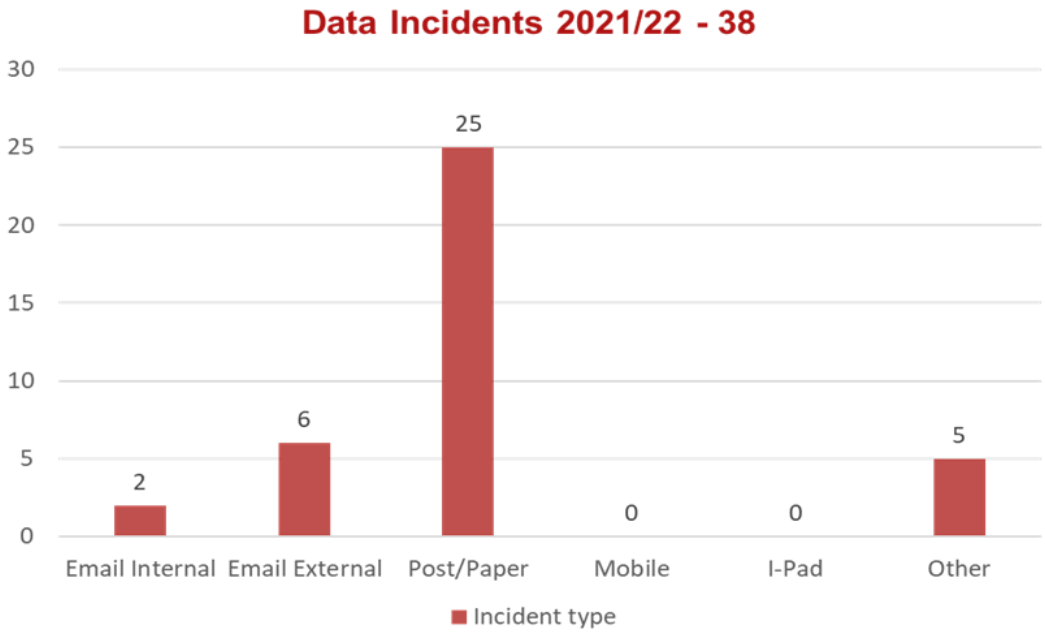


Appendix C Data Breaches

Emerging themes and planned improvements

- Paper / post continues to be highest source linked to breaches
- The introduction of the Revenues and Benefits team to the Corporate and Customer Services area has had an impact on the overall number of breaches due to the volume of paper / post created as part of their processes.
- 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 Data Protection Officer for overview and challenge as to remedial actions undertaken.
- The Information Governance team will create a generic data breach action plan to support the collation of root cause and remedial action evidence which will be rolled out across the authority by the end of September 2022.

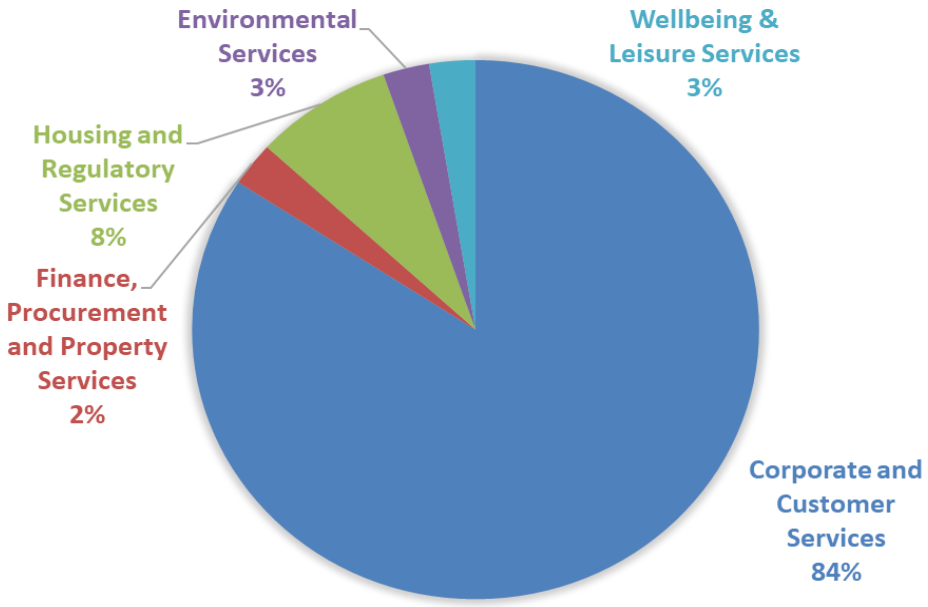
The following table shows the number of data breaches and the root cause for the period of 1st April 2021 – 31st March 2022.



The pie chart below represents the volume of data breaches per service area.

The highest volume of data breaches for 21 - 22 was reported by Corporate and Customer Services at 84%. This is a significant increase from the 15% reported in 20 - 21. The increase in part can be explained due to the transfer of the Revenue and Benefits team who were previously reported under Housing and Inclusion (as a third party supplier) who reported 53% of the overall breaches 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.



Learning continues to take place, which include 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 Data Protection Officer 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 reflected in the figures we see reported this year. It is imperative that services across the Council continue to develop and improve their processes around managing information and work with the Information Governance Officer to continue to embed best practices and protocols required.

We have introduced training, robust reporting and empowered staff across the Council to be proactive when a breach may occur, 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. Good information governance equals good cyber security – each element reduces the overall risk to information security.

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 Manager has collaborated with other teams on a broad range of projects and programmes across the Council, working to ensure that information security and data privacy 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.
- Attendance of the ICT Client Manager at the IG Committee 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 considerations are addressed in the early stages of a project, in line with legislation 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.