



Jacqui Sinnott-Lacey
Chief Operating Officer
52 Derby Street
Ormskirk
West Lancashire
L39 2DF

Thursday, 22 July 2021

**TO: COUNCILLORS E POPE, P O'NEILL, D DANIELS, I DAVIS, C DERELI,
A FENNELL, N FUREY, J GORDON, J MEE AND N PRYCE-
ROBERTS**

Dear Councillor,

SUPPLEMENTARY REPORT FOR AUDIT AND GOVERNANCE COMMITTEE – ITEM 8

Please find attached a report containing details of supplementary information prepared by the Corporate Director of Transformation and Resources, relating to item 8 on the agenda for the Audit and Governance Committee meeting, 28th July 2021.

Yours faithfully

A handwritten signature in black ink, appearing to be 'JS', written over a horizontal line.

Jacqui Sinnott-Lacey
Chief Operating Officer

**AGENDA
(Open to the Public)**

- 8. SENIOR INFORMATION RISK OFFICER ANNUAL REPORT APRIL 2020 - JULY 2021** 263 - 278
To consider the report of the Corporate Director of Transformation and Resources.

We can provide this document, upon request, on audiotape, in large print, in Braille and in other languages.

For further information, please contact:-
Kirsty Breakell on 01695 583312
Or email kirsty.breakell@westlancs.gov.uk



Audit and Governance Committee:

28 July 2021

Report of: Corporate Director of Transformation & Resources

Relevant Portfolio Holder: Councillor A. Yates

Contact for further information: Chris Twomey
(E-mail: chris.twomey@westlancs.gov.uk)

SUBJECT: Annual Report of Senior Information Risk Owner (SIRO)

1.0 PURPOSE OF THE REPORT

1.1 This report provides an overview of West Lancashire Borough Councils obligation in meeting statutory regulatory requirements relating to the processing of personal confidential or identifiable data under the UK General Data Protection Regulation, the Data Protection Act 2018 and our Councils duty to be transparent through compliance within the Freedom of Information Act 2000.

The report aims to provide sufficient information to the Audit and Governance Committee that highlights:

- The most significant current and emerging Data Privacy, Cyber Security and Information Governance (IG) issues
- Clarifies the measures being undertaken by the Council to ensure we meet both the national and mandatory compliance standards.

Specifically, the report will:

- Give an overview of key achievements in 2020/2021.
- Outline activity and performance related to information governance compliance during the reporting period for 2020 – 2021.
- Outline the Council's approach that underpins organisational compliance within the regulatory requirements relating to the handling of information and provide assurance of ongoing improvement in relation to risk management.
- Provide a status update on the Data Security and Protection Toolkit (DSPT).
- Detail how data incidents have been handled, including the learning from incidents.

Provide an overview of the priorities for compliance, within the Effective Data Management Programme for 2021/22.

2.0 RECOMMENDATIONS TO CABINET

2.1 That the respected Cabinet Members take note of this report.

3.0 RECOMMENDATIONS TO EXECUTIVE OVERVIEW & SCRUTINY COMMITTEE

3.1 That the respected Committee Members take note of this report.

4.0 Background

4.1 Information is an organisational asset and West Lancashire Borough Council (WLBC) must continue to embed a strong information governance culture, so that the Council continues to operate lawfully, efficiently and effectively.

The SIRO provides an essential role in ensuring that identified information security risks are followed up and incidents are managed and has ownership for the Information Risk Policy, Risk Management Strategy and associated processes. It is the SIRO's role to provide leadership and guidance to Information Asset Owners.

The responsibilities of a SIRO can be summarised as:

- Senior Information Risk Officer (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 Information Governance Manager, the Data Protection Officer and Information Asset Owners.

5.0 SUSTAINABILITY IMPLICATIONS

5.1 There are no significant sustainability impacts associated with this report and, in particular, no significant impact on crime and disorder.

6.0 FINANCIAL AND RESOURCE IMPLICATIONS

6.1 There are no significant financial or resource implications arising from this report.

7.0 RISK ASSESSMENT

7.1 This item is for information only and makes no recommendations. It therefore does not require a formal risk assessment and no changes have been made to risk registers.

8.0 HEALTH AND WELLBEING IMPLICATIONS

8.1 There are no health and wellbeing implications arising from this report.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and / or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

None



SENIOR INFORMATION RISK OFFICER ANNUAL REPORT April 2020 – July 2021

Purpose

This report provides an overview of West Lancashire Borough Council's obligation in meeting statutory regulatory requirements relating to the processing of personal confidential or identifiable data under the UK General Data Protection Regulation, the Data Protection Act 2018 and our Council's duty to be transparent through compliance within the Freedom of Information Act 2000.

The report aims to provide sufficient information to the Audit and Governance Committee that highlights:

- The most significant current and emerging Data Privacy, Cyber Security and Information Governance (IG) issues
- Clarifies the measures being undertaken by the Council to ensure we meet both the national and mandatory compliance standards.

Specifically, the report will:

- Give an overview of key achievements in 2020/2021.
- Outline activity and performance related to information governance compliance during the reporting period for 2020 – 2021.
- Outline the Council's approach that underpins organisational compliance within the regulatory requirements relating to the handling of information and provide assurance of ongoing improvement in relation to risk management.
- Provide a status update on the Data Security and Protection Toolkit (DSPT).
- Detail how data incidents have been handled, including the learning from incidents.
- Provide an overview of the priorities for compliance, within the Effective Data Management Programme for 2021/22.

Background

Information is an organisational asset and West Lancashire Borough Council (WLBC) must continue to embed a strong information governance culture, so that the Council continues to operate lawfully, efficiently and effectively.

The SIRO provides an essential role in ensuring that identified information security risks are followed up and incidents are managed and has ownership for the Information Risk Policy, Risk Management Strategy and associated processes. It is the SIRO's role to provide leadership and guidance to Information Asset Owners.

The responsibilities of a SIRO can be summarised as:

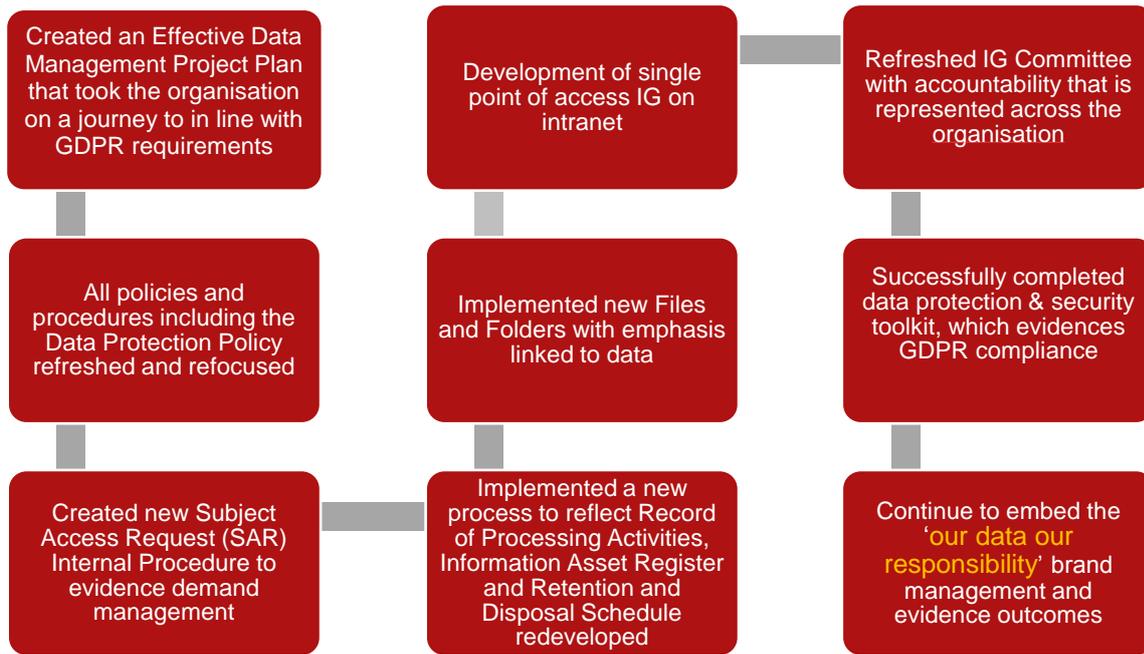
- Senior Information Risk Officer (SIRO) for the Council
- Lead Responsible Officer for fostering a culture that values, protects and uses information for the success of the organisation and benefit of its residents.
- Lead Responsible Officer for maintaining sufficient knowledge and experience of the 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 Information Governance Manager, the Data Protection Officer and Information Asset Owners.

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



Overview of key achievements in 2020/2021

The following graphic outlines the significant work that has been undertaken to ensure that the identified compliance actions have been achieved.



Outlined activity and performance related to information governance for the period 1st April 2020 – 31st March 2021

1. Freedom of Information Act 2000 (FOIA) and Environmental Information Regulation 2004 (EIR) requests for the period above was 663

FOI & EIR Requests 2020/21	Number of Requests received	% of responses within 20 working days	Number of requests were information was granted	Number of requests were information was refused	Number of internal reviews	Number of complaints to the ICO
Apr	46	96%	29	17	0	0
May	44	93%	29	15	2	0
Jun	52	90%	35	17	0	0
Jul	46	96%	39	7	0	0
Aug	58	86%	47	13	1	0
Sep	57	95%	50	7	0	0
Oct	70	97%	54	16	0	0
Nov	65	97%	48	17	2	0
Dec	47	96%	36	11	0	0
Jan	61	92%	60	1	0	0
Feb	68	94%	57	11	0	0
Mar	49	94%	42	7	1	0

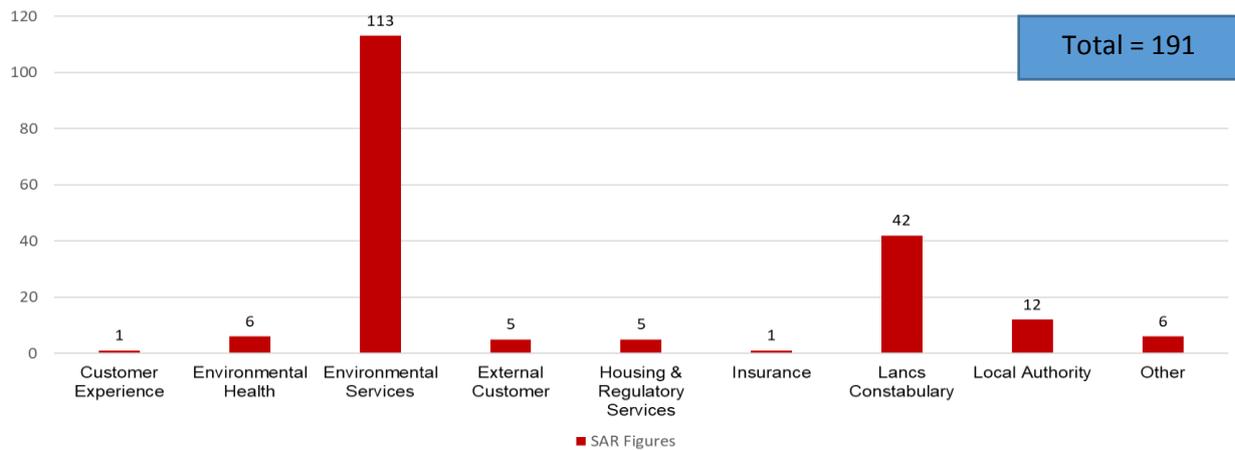
*Work underway to agree a reportable internal performance indicator.

Below is a list of themes, performance data and next steps:

- Of the overall FOI data requests, increases can be evidenced across Revenue & Benefits, Housing and Environmental services, linked to Covid statistic, benefit entitlement data and burial / cremation reports
- Continued focus on FOI performance has resulted in no action from the ICO
- Above 90% performance achieved consistently linked to the 20 day statutory time limit.
- August month performance dip was quickly identified and addressed
- 6 internal reviews were completed following the requester appeal of the initial FOI response. This review led to improved outcomes for the service attaining to vexatious FOI requests. In each case, as the requests were dealt with effectively, no further action was required in terms of reporting to the Information Commissioner's Office (ICO).

2. Requests for information under the Data Protection Act 2018 (Subject Access Requests)

The following table shows the number of Subject Access Requests (SAR) made under Data Protection legislation, for the period of 1st April 2020 – 31st March 21 reporting year.



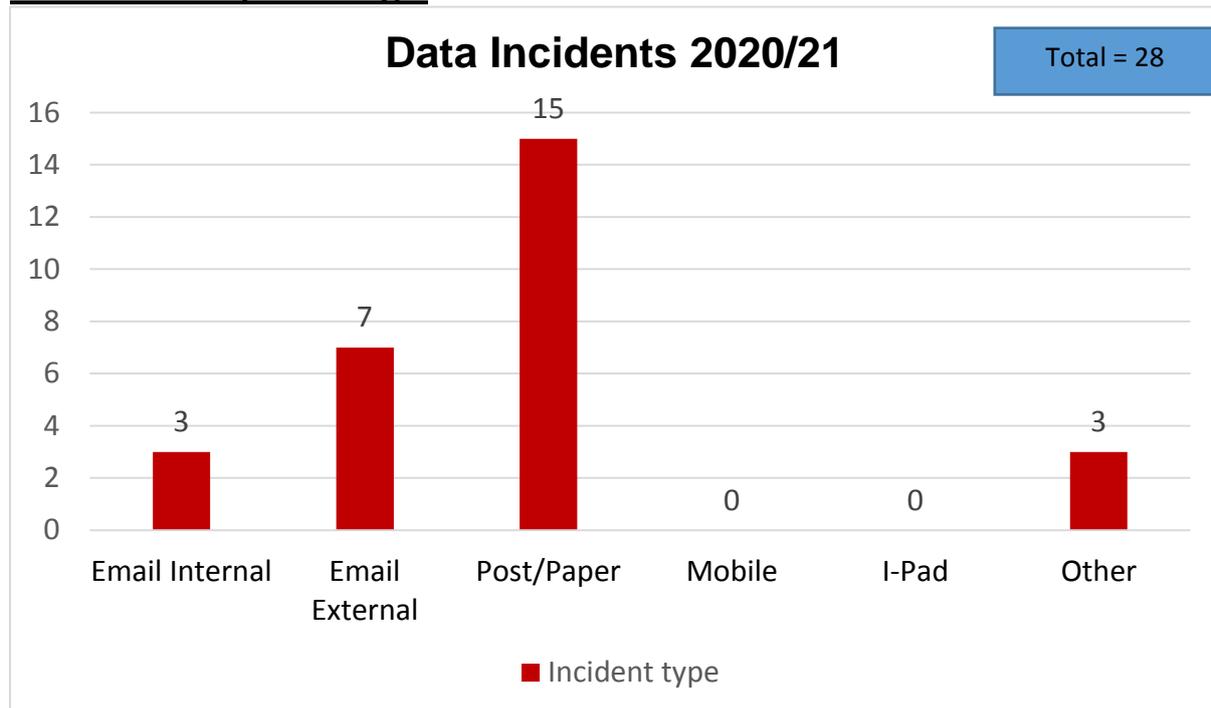
Below is a list of themes, performance data and next steps:

- Percentage of Subject Access Requests (SAR's) responded to within the performance measurement of a calendar month were **99%** with an average response time of 1 to 2 days.
- In 2020/ 2021 compared to 2019/2020 SAR's have increased by **40%** in areas such as Police requests, and other lawful requests by other local authorities
- To aid improved performance, a good practice SAR logging procedure has been introduced, allowing us to evidence demand management more robustly.
- Environmental services have seen an **80%** increase linked to enforcement protocols

3. Data breaches and self-referrals to the Information Commissioner's Office (ICO)

The following table shows the number of data breaches, self-referrals and source of breach to the ICO for the period of 1st April 2020 – 31st March 21 reporting year.

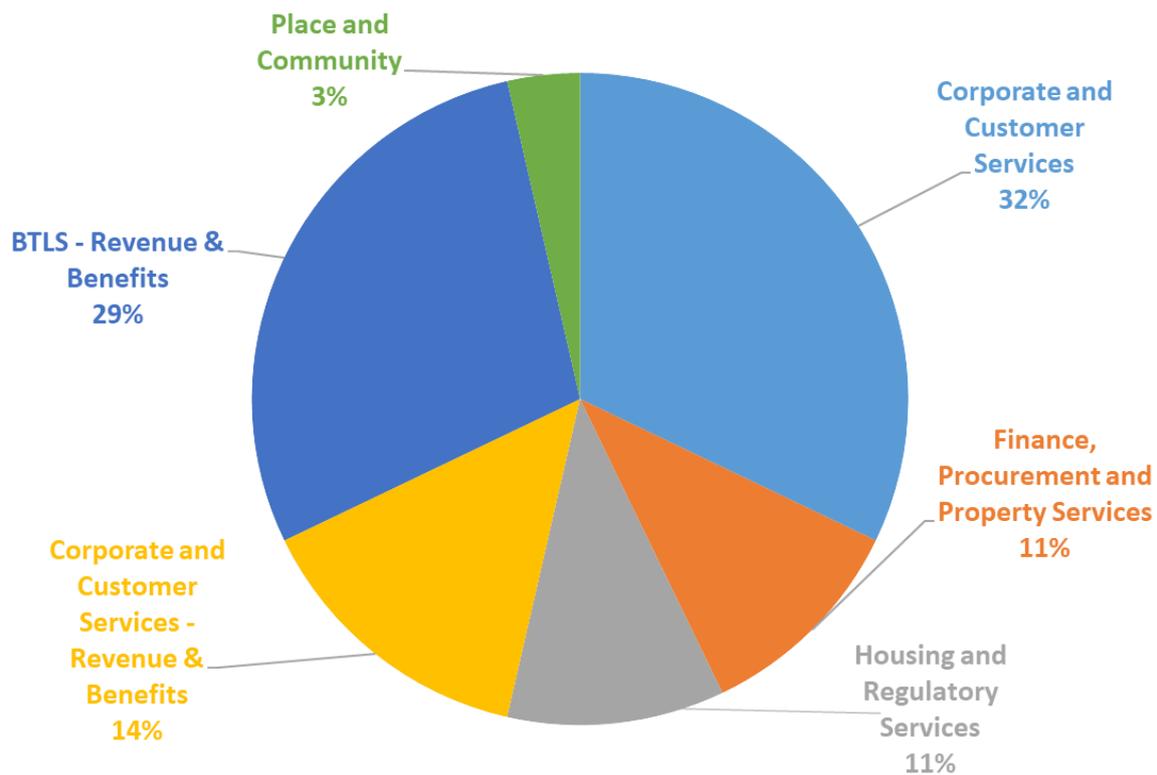
Data breaches by source type



Below is a list of themes, performance data and next steps:

- 100% of all data incidents were reported within the statutory 72 hours performance measurement.
- This is a significant improvement as 14 of the 48 incidents reported last year were over this timescale.
- The Data Breach procedure has been reviewed and refocused which has allowed us to evidence the diagnosis of incidents more robustly.
- 3 incidents reported to the ICO were due to the data being highly sensitive
- Highest proportion of incidents have been attributed to printing and mailing errors, which has been addressed via a remedial improvement plan with individuals and service areas

Data breaches per service area



The themes emerging are:

- Paper / post continues to be highest source linked to breaches
- Corporate and Customer services has seen the highest increase in comparison to the previous year. Revenue and Benefits now sit within the structure of Corporate and Customer Services. Prior to this Revenue and Benefits sat within BT Lancashire Services. The diagram above provides the percentage breakdown
- Significant support now in place, including a single point of access to subject matter experts, one to one support, development of remedial support and training plans and spot check monitoring to reduce risk to breaches re-occurring

Organisation compliance, risk management and continuous improvement

Changes to legislation during 2020/21

Regular monitoring of all legislation by the Data Protection Officer, has outlined that there have been no significant changes to primary legislation in the reporting period. We continue to learn how the new regulatory landscape post Brexit regarding data protection integrates with other activity.

We continue to monitor and share where necessary, guidance and developments from our Data Protection Officer (DPO) and the ICO.

Under the current Covid pandemic both legislation and working practices have further been developed to facilitate the exchange and sharing of personal data in support of dealing with

the emergency. The Council's Data Protection Officer (DPO) supported by the Business Intelligence and Development team have been actively engaged in putting together data sharing agreements in support of the Council's business activities related to Covid-19 .

The intention of the DPO this year is to focus on developing best practice tools, including:

- Introduction of a digital Data Protection Impact Assessment form
- Introduction of a new Information Governance E-learning platform
- Development of dynamic reporting linked to IG workforce training compliance
- Developing good practice guidance to support the completion of internal audits linked to compliance
- Strengthening accountability and governance linked to vendor security assessments within the architecture design authority
- Benefit realisation reporting via the Our Future Transformation board linked to the Effective Data Management Programme.

Update status on the NHS Data Security and Protection Toolkit (DSPT)

NHS Data Security and Protection Toolkit

As we continue to strengthen our partnership working, and to support us to deliver the aspirations outlined within our Corporate plan, it is key that any data sharing is done within a compliant framework. During Covid-19 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 and how, we as an organisation, in collaboration with partners, the Council could target a range of intervention measures that would reduce risk and support our residents to access services at a place based level that aimed to support their health and wellbeing..

To maintain the highest standards of data privacy for all data shared with the NHS and partners, we have recently completed our first submission of the NHS Data Security and Protection Toolkit (NHS DSPT).

The online self-assessment tool, which evaluates the performance of our organisation against the ten data security standards outlined by the National Data Guardian.

It is a requirement for any organisation that has access to NHS patient data to submit a response. This provides the NHS and other partner organisations with the assurance that all personal data is being managed securely and handled in line with legislation.

During May and June 2021, a project team consisting of officers from the BID Team, Internal Audit, HR, and Procurement, along with other services, worked together to gather evidence in support of each of the detailed assertions.

This was a significant piece of work, as we strived to evidence compliance against these standards.

Following our submission, we have achieved a compliant status, which was excellent news for the Council.

Data Incident Analysis

1. 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 Ministry of Housing, Communities and Local Government (MHCLG) leading the way with guidance, training and action plans aimed specifically at organisations such as our Council.

The Council's IT and Cyber Security services have been outsourced to Lancashire County Council (LCC) which was previously managed by BT Lancashire Services (BTLIS). It is LCC's responsibility to ensure our council's IT infrastructure has robust policies and procedures in place to help wherever possible prevent attacks against our corporate data or employees and customers.

2. Data breach reporting

We have introduced 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 as part of continuous improvement.

Colleagues are encouraged to share their concerns and seek advice. Good information governance results in good cyber security – each element reduces the overall risk to information security.

Cyber Security is not just LCC's responsibility – good recovery is achieved by senior managers using their knowledge of their information and systems and working with ICT and our 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 and risks are mitigated as new and more efficient ways of working are introduced. This has included:

- Working with the procurement and the legal team on a best practice approach to tendering
- 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 any project, in line with legislation and ICO expectations.

3. Information sharing requests

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.

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.

4. Data Incidents

Within the report, it has been highlighted that during 2020/21 there had been **28** breaches. Much learning has taken place as a result of these, the team has developed and implemented a number of tools and measures which aim to improve our overall information governance and cyber-security.

The Information Governance Manager and Data Protection Officer has 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. The information governance link officers within each service area and the Information governance committee are key networks that ensure the Council continues to develop and improve their processes around managing information and to continue to embed best practices and protocols required.

5. Reporting

Whilst it is clear that the Council is responsible for high volumes of data, a key focus of work this year has been to deliver the GDPR audit report recommendations, whilst establishing an understanding of demand management linked to Information Governance requirements.

The introduction of new ways of working, including workflow solutions have now enabled the Council to gain insight into the current state regarding all compliance work demands.

The data captured will continue to be utilised to create more dynamic reporting for the forthcoming year.

This approach will allow information governance data to be used to influence and shape strategic and operational decision making that will continuously improve compliance performance, underpinned by the introduction of new key performance indicators.

West Lancashire Borough Council Continuous Improvement Plan 2021/22 within the Effective Data Management Programme

