CYNGOR
monmouthshire
COUNTY COUNCIL
sir fynwy

REPORT

SUBJECT:	**Freedom of Information (FOI) and Data Protection Act (DPA) Breaches & Data Subject Access Request (DSARs) Report**
MEETING:	**AUDIT COMMITTEE**
DATE:	**20th June 2022**

1. PURPOSE:

1.1 The purpose of this report is to describe how we respond to our legal responsibilities to manage our information resources under the Freedom of Information (FOI) and Data Protection Act (DPA). We will also present you with relevant performance statistics for you to evaluate.

2. RECOMMENDATIONS

2.1 Members are asked to scrutinise the report and request any clarification of the information within it. We also invite members to discuss how we could improve the layout of the stats or the level of detail in order to make the data more useful and meaningful.

3. KEY ISSUES:

3.1 Information is the lifeblood of the organisation, and without it we cannot undertake any of our normal day to day duties as a council. It is a valuable resource on a par with money and people. It needs to be kept safe and secure at the same time as making it available to the right person at the right time and the right place.

3.2 MCC administers its information resource within the Information Security and Technology Team (ISTT). It is headed by the Senior Information Risk Officer (SIRO) and is responsible for cyber security as well as making sure we comply with legislation.

3.3 The legal responsibilities for information management are under the Freedom of Information and Data Protection Acts, and non-compliance with the legislation can result in financial penalties in severe cases. However, any financial penalties we incur are not as damaging as the disruption to our operational services or the loss of personal data.

3.4 The majority of our information is held in digital format, and modern flexible working practices have increased risk of data loss from cyber-crime or human error. Where personal information is compromised it’s called a data breach, and there are protocols to follow to minimise the effects, or harm, to the people concerned.

3.5 The ISTT also manages the transition from paper to digital storage and ensures that digital storage is organised and managed so that it can be easily available to the right person, in the right format and at the right time.

3.6 The statistical data included in this report isn't just for information. It is actively used by the ISTT to target changes in the way we record information, making it easier to extract the relevant data on request. It is also used to assess the training needs of the organisation and to focus that training to services with a higher risk of a data breach.

3.7 A meeting of the Information Governance Group is held on a quarterly basis. The group is made up of representatives from each Directorate who oversee any changes to the way data is stored, used and published. A full report on Freedom of Information requests, Data Breaches and Data Subject Access requests are presented to this group for scrutiny.

4. FREEDOM OF INFORMATION

4.1 The Freedom of Information Act 2000 allows anyone to request any data and information held by the council, whether stored electronically or on paper. The Act imposes certain timescales and conditions around the format and supply of information. The Information Governance Officer oversees the management and co-ordination of FOI requests, though the information must be collated and supplied by service areas within the statutory deadlines. Such is the workload of FOI requests, the council have recruited an Information Governance Coordinator to support the management of this area, along with other Information Security and Technology tasks.

4.2 An internal review is conducted where the requestor is not satisfied that a full response has been given. The review covers internal processes used to uncover the information, as well as deciding whether the statutory regulations have been met. The number of these in the last year is documented below.

4.3 Requests under FOI and Environment Information Request (EIR) are not currently segregated. Figures include both. From April 2022 the statistics for FOI and EIR have been separated and subsequent reports will reflect this. The target is for a percentage of FOI's closed within 20 Working Days. The target of 90% closed requests was not achieved for the financial year 2021/22. This is, in the main part, due to the Covid-19 response and many service areas working with reduced staffing.

4.4 The number of requests received by Monmouthshire in recent years are documented in the following table. All statistics related to FOI compliance are now published on the FOI page of the Corporate website.

Financial Year	Number of requests received
2015-16	1061
2016-17	1045
2017-18	1005
2018-19	No statistics available
2019-20	931
2020-21	796
2021-22	932

4.4.1 **Breakdown of last financial year (April 2021 to March 2022)**

	2019/20	**2020/21**	**2021/22**
Requests received	931	796	932
Requests closed on time	619 (69%)	394 (50%)	685 (73%)
Internal Reviews	3	5	11

4.4.2 Current overview of this calendar year (2022):

1st January 2022 - 5th May 2022

Requests received	353
Requests closed	285/305
Requests closed on time	93%
Internal Reviews	3

This recent data shows a very positive trend in the number of FOIs closed on time.

4.5 FOI requests are now allocated into the service areas that ‘own’ the response by the statutory deadlines. This is to help Members identify where the FOI requests are targeted, and where we may store information differently to help people to self-serve.

Service Area	**Number of requests (2020/21 Financial year)**	**Number of requests (2021/22 Financial year)**
Chief Executives	37	n/a
Children and Young People	34	49
Enterprise (Majority are planning)	205	255
Mon Life	8	15
People & Governance (2022)	n/a	17
Policy, Performance & Scrutiny (2022)	n/a	37
Resources	282	259
Social Care, Health and Safeguarding	200	225
Other	30	75

4.6 It should be noted that though the administration of FOI’s rests within the ISTT it is the responsibility of the service departments to collate the information required by the FOI. The Information Governance Officer has met with various service area leads to address the need for prompt action.Bespoke training is now being administered to specific service areas so that any issues with answering FOI/EIR requests can be addressed.

4.7 Many service areas were impacted by the response to Covid-19 and this was particularly noticeable in FOI return times. The Information Commissioner’s Office issued statements allowing Local Authorities to ‘relax’ response times whilst still urging a need for replies to be sent in a timely manner.

4.8 The Information Governance Officer introduced measures to recover from the Covid backlog over the past two years. Requesters with outstanding requests were contacted to ascertain whether they still wanted the data. Enquirers were given set time scales to respond before the requests were closed unanswered. Figures for this can be found on the FOI Compliance Data, published on the FOI webpage (as above).

4.9 Considerable effort is being made to ‘signpost’ people to readily available information rather than respond in detail to an FOI request. This is linked to opening up our data on our website in order for people to self-serve.

5. DATA PROTECTION ACT BREACHES

5.1 The Data Protection Act 2018 is there to ensure we secure our data from theft, loss or mismanagement. From time-to-time data breaches may occur which could have a harmful effect on an individual and these breaches must be managed to ensure they can’t re-occur and to minimise any damage that has occurred. The ‘more serious’ breaches are reported to the Information Commissioner’s Office (ICO), and these are included in this report for analysis.

5.2 **Tables i** & **ii** below set out the number of breaches split into directorates and type. It is useful to note that the whole council is classed as a single ‘data controller’, whilst each school is its own ‘data controller’ so is responsible for its own data protection management.

Table i - Number of Data Breaches recorded 1st April 2021 to 31st March 2022 (all data in the subsequent tables refer to data collected between these dates)

Directorate	**Number of Data Breaches**
Chief Execs	2
Children & Young People	10
Enterprise	6
Resources	6
Schools *(own Data Controllers)*	16
Social Care, Health & Safeguarding	29
TOTAL	**69**

Table ii - Type of data breach

Cyber Security Issue	0
Email**	55
Paper Records	3
Laptop/other devices	0
Other*	11
TOTAL	**69**

* ’*Other’ breaches include electronic records shared or accessed incorrectly, records not redacted accurately, or photographs being shared without consent*

*** Emails account for 80% of all breaches in 2021/22. This is an increase from 75% the previous year (2020/21) and 65% in the year before that (2019/20).*

Table iii - Number of Data Breaches reported to the ICO

Corporate	3
Schools	0
TOTAL	**3**

The Data Breaches that were reported to the ICO in **Table iii** did not result in any penalties or sanctions by them. When responding, the ICO issued a 'checklist' to support learning and training of staff with no further action from themselves.

Table iv - Number of Data Incidents ('near miss breaches)

Corporate	7
Schools	1
TOTAL	**8**

The Data Incidents referred to in **Table iv** relate to issues that have occurred where some personal data may have been compromised or lost but has not resulted in a breach. For example, an attachment being sent to the incorrect email address, but the password for the attachment was not shared, would be recorded as an 'incident' as no personal data was accessed by an incorrect recipient.
These Data Incidents, or 'near misses' provide good learning opportunities for staff to reflect on practices and can often instigate change in a process to ensure a breach is not incurred in future.

5.3 Since April 2021, we have recorded data breaches/incidents caused by other organisations that contain MCC data. For example, a member of a Health Board sharing a MCC care report with an incorrect person which resulted in a breach of personal data. These breaches are following up robustly with the external organisation and recorded for reference purposes.

Table v - Number of External Organisation Breaches and Incidents

Corporate	6
Schools	1
TOTAL	**7**

5.4 A new process has been introduced for Data Protection Impact Assessments (DPIA) to be drawn up when services adopt new systems to ensure we are considering the implications of the data protection principles. These are being compiled into a DPIA register so an overview of all processes and new risks can be accessed efficiently.

5.5 Updated Mandatory online GDPR training was launched in November 2021 and the uptake of this training is reported to the Information Governance Group. This training should be carried out every two years. **Table vi** shows how many members of staff have completed this training in the seven-month period since it was launched.

Table vi - GDPR Mandatory Training (November 2021 to May 2022)
By Directorate:

Chief Execs	69
Children & Young People*	141
Enterprise (inc. Mon Life)	166
MonLife	172
People & Governance	58
Resources	89

Social Care, Health & Safeguarding	331
TOTAL	**1026**
Schools**	**398**

NB ** contains some School Staff*
*** one Secondary School completed with an External training company*

6. DATA SUBJECT ACCESS REQUESTS

6.1 Individuals have the right to request to see any personal information that's held on them by the council. These Data Subject Requests (DSARs) require the council to search for any records they may hold, and make sure anyone else's personal information is redacted. The vast majority of DSARs relate to Social Care and, because these records can go back many years, responding to these requests is quite an undertaking. The number of DSARs therefore may not reflect the resources needed to collate the information.

6.2 For the purposes of this report, the number of DSARs received and responded to has is shown in the table at 5.4. This includes a breakdown of the main request service areas.

6.3 Financial Year 2019/20 - 51 DSARs
Financial Year 2020/21 - 49 DSARs
Financial Year 2021/22 – 61 DSARs (*may not be final figure due to open cases)

6.4 **Number of Data Subject Access Requests for Financial Year 2021/22 (as current data stands)**

Data Subject Access Requests	**2020/21 Number**	**2021/22 Number**
Children's Services	31	41
Adult Services	6	4
Mixed Children's and Adult Services	3	2
Whole Authority	9	14
TOTAL	**49**	**61**
Number of individual requestors above	*41*	*47*
Number of 'on time' replies (28 days)	*57%*	*59%*
Number of enquiries received (Missing Persons/Proof of Life etc.)	***13***	***6***

7. CONSULTEES:

Information Security and Technology Team
Chief Officer Resources

8. BACKGROUND PAPERS:

FOI requests, DPA breach notifications & DSARs records

AUTHOR: Sian Hayward – Head of Information Security and Technology & SIRO
CONTACT DETAILS:
Tel: 01633 344309 / 07971893998
Email: sianhayward@monmouthshire.gov.uk