REPORT

SUBJECT: Annual report of Freedom of Information (FOI), Data Protection Act (DPA) Breaches, Data Subject Access Request's (DSAR's)

MEETING: AUDIT COMMITTEE

DATE 29th June 2023

1. PURPOSE:

1.1 The purpose of this report is to inform members of how we manage our legal responsibilities towards the Freedom of Information (FOI) and Data Protection Act (DPA). These responsibilities are met wholly by the actions of staff and the policies and procedures that are in place. We will also present you with relevant performance statistics for you to evaluate.

2. RECOMMENDATIONS

2.1 Members are asked to scrutinise to review and assess the Council's arrangements for managing and responding to information requests and breaches and to consider the adequacy and effectiveness of those arrangements.

3. KEY ISSUES:

3.1 Information is a key resource alongside finance and people. Our use, storage and publication of information is governed by legislation in the form of the Freedom of Information and Data Protection Acts. Non-compliance with this 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.

3.2 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.

3.3 The statistical data included in this report isn't just for information. It is actively used 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.

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.

4.2 All processes and procedures surrounding Freedom of Information within the Authority were subject to an Internal Audit review in June 2022. This was completed very successfully and very few minor recommendations were made. The report from this audit was noted and reported back to the Information Governance Group.

4.3 Requests under FOI and Environment Information Regulations (EIR) have been segregated for the year ended March 2023. Environmental Information Requests differ from Freedom of information in that they relate to any information that impacts our surroundings e.g. planning and highways. There are also differences in the way that we deal with the requests from a legislative point of view.

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**
2019-20	931
2020-21	796
2021-22	932
2022-23	992 (250 EIR, 742 FOI)

4.4.1 **Breakdown of last financial year (April 2022 to March 2023)**

	2019/20	**2020/21**	**2021/22**	**2022/23**
Requests received	931	796	932	992
Requests closed on time	619 (69%)	394 (50%)	685 (73%)	909 (92%)
Internal Reviews	3	5	11	19

4.4.2 Internal Reviews (IR) are undertaken when the council has failed to provide FOI information within the legislative timescales or where the requestor believes we have sent inaccurate or incomplete information.

Members will note an increase in the number of Internal Reviews over the last 4 years. This is because:

- The FOI/EIR requests received are more complex and therefore take more time and resource to complete them.
- The FOI team actively promote the IR facility in order to ensure we assist members of the public to understand what we are able to do under the specific legislation and to help them find an informal resolution to their query before it is escalated to the ICO.

4.4.3 **Current overview of this calendar year (2023):**

1st January 2023 - 19th May 2023

Requests received	423
Requests closed	379
Requests closed on time	354 (93%)
Internal Reviews	8

This recent data shows a very positive trend in the number of FOIs closed on time. Closed requests have increased from 73% to 92% in the last year.

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)**	**Number of requests (2022/23 Financial year)**
Chief Executives	37	n/a	n/a
Children and Young People	34	49	64
Enterprise (now Communities & Place)	205	255	297
Mon Life	8	15	21
People & Governance (2022)	n/a	17	67
Policy, Performance & Scrutiny (2022)	n/a	37	65
Resources	282	259	233
Social Care, Health and Safeguarding	200	225	213
Other	30	75	32

4.6 It should be noted that though the general administration of FOI's rests within the Information Security & Technology (IST) team, it is the responsibility of the service departments to search for, collate and redact any personal information before it is submitted to the requestor. 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 The IST team has cleared the backlog created by Covid, whilst continuing with 'business as usual' and increasing its performance with response times.

4.8 Considerable effort is being made to 'signpost' people to readily available information rather than respond in detail to an information 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 Breaches can be reported to us from internal or external sources and in any way. We actively encourage breach reporting *of any kind* in order for us to evaluate whether they are serious or not. We don't expect people to have that degree of knowledge of what constitutes a breach. Once reported, breaches are documented and categorized.

5.3 The tables 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 iii shows the number of breaches notified to the ICO

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

Directorate	**Number of Data Breaches**	
	2021/22	**2022/23**
Chief Execs	2	3
Children & Young People	10	12
Enterprise (Communities & Place)	6	13
Mon Life	n/a	4
People & Governance	n/a	3
Policy, Performance & Scrutiny	n/a	1
Resources	6	0
Schools *(own Data Controllers)*	16	21
Social Care, Health & Safeguarding	29	32
TOTAL	**69**	**89**

Table ii - Type of data breach

	2021/22	**2022/23**
Cyber Security Issue	0	0
Email**	55	70
Paper Records	3	11
Laptop/other devices	0	0
Other*	11	8
TOTAL	**69**	**89**

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

*** Emails continue to account for a high proportion (79%) of all breaches in 2022/23.*

Table iii - Number of Data Breaches reported to the ICO

	2021/22	2022/23
Corporate	3	2
Schools	0	0
TOTAL	**3**	**2**

5.4 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)

	2021/22	2022/23
Corporate	7	19
Schools	1	1
TOTAL	**8**	**20**

5.5 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.

5.6 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. It is pleasing that more incidents of this nature are being reported so that the cause of these can be investigated.

5.7 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 followed up robustly with the external organisation and recorded for reference purposes.

Table v - Number of External Organisation Breaches and Incidents

	2021/22	2022/23
Corporate	6	5
Schools	1	2
TOTAL	**7**	**7**

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

6. TRAINING

6.1 GDPR (General Data Protection Regulations) and Data Protection Training is mandatory for all staff and must be completed every two years. This satisfies ICO's guidelines. In practice, we fail to achieve 100% of this target, with 78% undertaking the training in the last two years. In order to address the short fall, we concentrate on high-risk areas where sensitive information is being held and a high level of breaches occur.

6.2 This training is in the format of an online presentation and brief 'quiz' to check that employees actually understand the training provided rather than ticking a box.

6.3 Over the coming months, a new I.T. system for staff learning is being launched. This is an online learning management platform called 'Thinqi' and it is a very robust way of providing all staff with a wide range of suitable training opportunities, as well as allowing managers to track who has completed mandatory training. The GDPR/DP training has already been converted into the correct format for 'Thinqi' and is currently being trialed.

6.4 Other training provided for staff by the IST team (often face to face) includes bespoke sessions covering FOI/EIR, personal data redaction and any other aspects of GDPR or data protection as required.

7. DATA SUBJECT ACCESS REQUESTS

7.1 Individuals have the right to request to see any personal information that's held about 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 Council has one month to do this. 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. The volume of requests has increased by 54% in the last financial year and is becoming even more resource intensive.

7.2 Requests are received externally via the contact centre or through the website. All requests are recorded and sent to the pertinent service to process.

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

7.4 Financial Year 2019/20 51 DSARs
Financial Year 2020/21 49 DSARs
Financial Year 2021/22 61 DSARs
Financial Year 2022/23 94 DSARs

7.5 **Number of Data Subject Access Requests for Financial Years (as current data stands)**

Data Subject Access Requests	**2020/21 Number**	**2021/22 Number**	**2022/23 Number**
Children's Services	31	41	69
Adult Services	6	4	9
Mixed Children's and Adult Services	3	2	10
Whole Authority	9	14	6
TOTAL	**49**	**61**	**94**
Number of individual requestors above	*41*	*47*	*67*
Number of 'on time' replies (28 days)	*57%*	*59%*	*64%*
Number of enquiries received (Missing Persons/Proof of Life etc.)	***13***	***6***	***11***

8. CONSULTEES:

Information Security and Technology Team
Chief Officer Resources

9. 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**