REPORT

SUBJECT: Annual report of Freedom of Information (FOI), Data Protection Act (DPA) Breaches, Data Subject Access Requests (DSARs)

MEETING: AUDIT COMMITTEE

DATE 6th June 2024

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 Under the Freedom of Information Act (FOIA) 2000 and Environmental Information Regulations (EIR) 2004, members of the public are entitled to request copies of recorded information that the Council holds.

Requests can be for any information we hold. EIRs are requests for environmental matters. Information held may be in digital form, paper form or recordings. We do not have to create information if it is not held at the time of request.

Requests may be received via the Contact Centre, website, email, social media or written letter. EIRs can also be submitted verbally. FOIs and EIRs can be received by any member of staff and should be forwarded to the FOI team.

Once received by the Council, we have 20 working days to provide the response, if held, or to supply a refusal. It is the responsibility of the service departments to search for, collate and redact the information before it is submitted to the requestor.

We can only refuse to disclose information if it is covered by an exemption (FOI) or exception (EIR). Examples include personal data of third parties, safeguarding security, disclosure would adversely affect and course of justice.

Some FAQ datasets are held on our website for ease of responding to common themes.

Responses are normally sent in the same manner as request received – email, post etc. Enquirers can request alternative formats and methods of return.

If an enquirer is dissatisfied with the response, they can request an Internal Review which is carried out by the Senior Information Risk Officer (SIRO).

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.

4.4.1 **Breakdown of last financial year (April 2023 to March 2024)**

Financial Year	Number of requests received
2020-21	796
2021-22	932
2022-23	992 (250 EIR, 742 FOI)
2023-24	1159 (292 EIR, 867 FOI)

	2020/21	2021/22	2022/23	2023/24
Requests received	796	932	992	1159
Requests closed on time	394 (50%)	685 (73%)	909 (92%)	1069 (92%)
Internal Reviews	5	11	19	25

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 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.
- A significant number of these reviews have been requested by a single enquirer.

4.4.3 **Current overview of this calendar year (2024):**

1st January 2024 - 16th May 2024

Requests received	423
Requests closed	381
Requests closed on time	361 (95%)
Internal Reviews	8
Informal Responses*	57

**These queries were closed by FOI team as 'course of business' to reduce the administrative burden of departments.*

4.5 FOI requests are 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 (2023/24 Financial year)**
Communities & Place	332
Children and Young People	97
Mon Life	52
Other (inc. Whole Org.)	42
People & Governance	58
Law & Governance (2024)	5
Policy & Performance	48
Resources	221
Social Care, Health and Safeguarding	304
TOTAL	**1159**

4.6 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 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. It should be noted that, up to 16th May 2024, the FOI team have responded (in full or part) to 32% of total information requests themselves.

5. DATA PROTECTION ACT BREACHES

5.1 Under Article 33 of the UK GDPR 21018, the Council must report any breaches of data to the supervisory authority unless it is unlikely to result in a risk to the rights and freedoms of natural persons. The supervisory authority for the Council is the Information Commissioner's Office (ICO).

All staff are asked to alert the Data Protection Officer if they suspect a breach of personal data. This information is assessed as to whether it is an actual breach and if there is any potential 'harm' to the person (the data subject) whose information has been shared in error.

All potential breaches are investigated thoroughly and logged alongside any relevant information. If it is necessary to report the breach to the ICO, then this must be done within 72 hours of being alerted to the issue. The ICO then make a judgement as to whether the breach was preventable and whether all preventative steps had been taken. They also have the power to issue fines if a serious infringement has occurred. They may, alternatively, issue warnings, reprimands or recommendations.

If a person or organisation has received any personal data of another person/s in error, then they are asked to return, delete or destroy that data. They are also asked to sign a containment form to confirm this.

In most cases, the data subject is also informed that the breach has occurred.

5.2 Breaches can be reported to us from internal or external sources and in any way. We encourage breach reporting of any kind so we can 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**	**2023/24**
Chief Execs	2	3	1
Children & Young People	10	12	10
Enterprise (Communities & Place)	6	13	10
Mon Life	n/a	4	1

People & Governance	n/a	3	2
Policy, Performance & Scrutiny	n/a	1	2
Resources	6	0	0
Schools *(own Data Controllers)*	16	21	16
Social Care, Health & Safeguarding	29	32	24
TOTAL	**69**	**89**	**66**

Table ii - Type of data breach

	2021/22	**2022/23**	**2023/24**
Cyber Security Issue	0	0	0
Email**	55	70	52
Paper Records	3	11	3
Laptop/other devices	0	0	0
Other*	11	8	11
TOTAL	**69**	**89**	**66**

* '*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 2023/24. This is minor in proportion to the millions of emails sent from MCC accounts each year.*

Table iii - Number of Data Breaches reported to the ICO

	2021/22	**2022/23**	**2023/24**
Corporate	3	2	1
Schools	0	0	0
TOTAL	**3**	**2**	**1**

5.4 The Data Breach that was 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**	**2023/24**
Corporate	7	19	31
Schools	1	1	3
TOTAL	**8**	**20**	**34**

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 Records are kept of 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. For service areas who deal with a large amount of personal data, bespoke face to face training is also provided.

Table v - Number of External Organisation Breaches and Incidents

	2021/22	**2022/23**	**2023/24**
Corporate	6	5	7
Schools	1	2	1
TOTAL	**7**	**7**	**8**

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.

6. DATA SUBJECT ACCESS REQUESTS

6.1 Under Article 15 of the UK GDPR 2018, an individual is entitled to receive a copy of any records containing their personal data that are held by the Council.

Requests may be received via the Contact Centre, website, email, written letter or via a conversation with a member of staff.

Personal detail collection forms are sent to the requester to confirm their identification.

On receipt of confirmed identification, the Council have one calendar month to respond to the requester. All requests are recorded and sent to the pertinent service to process.

Records that contain third party information need to be redacted so that this information is not visible to the requester.

The records may be returned to the requester in paper or electronic format. This is agreed with the requester at the start of the process.

6.2 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 significantly in the last two financial years and is becoming even more resource intensive.

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

6.4 Financial Year 2020/21 49 DSARs
Financial Year 2021/22 61 DSARs
Financial Year 2022/23 94 DSARs
Financial Year 2023/24 108 DSARs

6.5 **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	2023/24 Number
Children's Services	31	41	69	57
Adult Services	6	4	9	16
Mixed Children's and Adult Services	3	2	10	4
Whole Authority	9	14	6	31
TOTAL	**49**	**61**	**94**	**108**
Number of individual requestors above	*41*	*47*	*67*	*88*
Number of 'on time' replies (28 days)	*57%*	*59%*	*64%*	*65%*
Number of enquiries received (Missing Persons/Proof of Life etc.)	***13***	***6***	***11***	***31***

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 / 07971 893998
Email: **sianhayward@monmouthshire.gov.uk**