REPORT

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

MEETING **AUDIT COMMITTEE**

DATE **4th June 2026**

1. PURPOSE

1.1 The purpose of this report is to inform members of the committee of how the Council manages its legal responsibilities towards the Freedom of Information Act (FOIA) and Data Protection Act (DPA). These responsibilities are met wholly by the actions of staff and the policies and procedures that are in place. The report also presents relevant performance statistics for the committee to evaluate.

2. RECOMMENDATIONS

2.1 Members are asked to scrutinise, 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. The 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 that the Council incur are not as damaging as the disruption to operational services or the loss of personal data.

3.2 The majority of 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 information is recorded, 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 held. EIRs are requests for environmental matters. Information held may be in digital form, paper form or recordings. The Council do not have to create information that 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, the Council has 20 working days to provide the response 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.

The Council 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. A public interest test (PIT) is often required to apply exemptions/exceptions.

Some FAQ datasets are held on the website for ease of responding to common themes. These are updated quarterly by the FOI team.

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, the FOI team will try to resolve informally in the first instance. If the enquirer remains unsatisfied, they can request an Internal Review which is carried out by the Information Management and Governance Lead Officer.

The number of requests received by Monmouthshire County Council in recent years are documented in the following table. It should be noted that FOI/EIR requests received have become more complex and therefore take more time and resource to complete them.

All statistics related to FOI compliance are published on the FOI page of the Corporate website.

4.2 **Breakdown of last financial year (April 2025 to March 2026)**

Financial Year	Number of requests received
2022-23	992 (250 EIR, 742 FOI)
2023-24	1159 (292 EIR, 867 FOI)
2024-25	1021 (217 EIR, 804 FOI)
2025-26	1058 (265 EIR, 793 FOI)

	2022/23	2023/24	2024/25	2025/26
Requests received	992	1159	1021	1058

Requests closed on time	909 (92%)	1069 (92%)	979 (96%)	985 (93%)
Internal Reviews	19	25	15	41

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

4.3.1 Members will note an increase in the number of Internal Review requests in the last year. The Council are receiving a significant number of Internal Review requests generated by enquirers using AI, which contributes to this increase. A number of enquirers also submit multiple requests in short succession and request an IR on each of them. As examples, 5 of the Internal Review in year were submitted individually by a single enquirer within a 2 week period. A further 5 were requested by a different enquirer on a single email, listing 5 references they wanted to contest at once. These needed to be registered separately against each reference, though they were handled together.

4.3.2 Where possible, a portion of requests are being handled by the team informally under course of business, rather than registered formally under FOI/EIR legislation. This practice started in 2024/25 and accounts for the drop in total requests received from that year.

Requests for standard, readily available information (such as a request for the name and email of the Chief Executive) are handled informally.

Handling a request informally deceases administrative burden to the team, and allows them to provide more prompt, helpful responses to the enquirers. Alongside the informal response, the offer to handle each request formally is provided to ensure legislative requirements are met. This approach has had positive feedback, with multiple compliments to the team for their speed of response.

Requests handled informally	Number
2024/25	213
2025/26	242

4.4 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.

Service Area	**Number of requests (2023/24 Financial year)**	**Number of requests (2024/25 Financial year)**	**Number of requests (2025/26 Financial year)**
Communities & Place	332	309	336
Children and Young People	97	101	95
Mon Life	52	46	48
Other (inc. Whole Org.)	42	38	35
People & Governance	58	N/A	N/A
Law & Governance (2024)	5	25	20
Policy & Performance	48	72	89
Resources	221	216	187
Social Care, Health and Safeguarding	304	214	248
TOTAL	**1159**	**1021**	**1058**

4.5 The Information Governance Officers provide FOI/EIR training where required, with a focus on high-demand and front-line teams.

4.6 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 data on the website in order for people to self-serve. It should be noted that in 2025/26 the FOI team have responded (in full or part) to 12.9% of formal requests themselves, or 29.2% of all requests if including informal responses.

5. DATA PROTECTION ACT BREACHES

5.1 Under Article 33 of the UK GDPR 2018, 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. The ICO 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.

All staff receive mandatory GDPR/Data Protection training and this is available on the Thinqi Learning Management System as part of the 'Essential Learning' package for all staff. This has recently been updated (17/04/2026) and relaunched. It is predicated that, within the next few months, nearly all staff will have completed. The system is set up with robust 'chasing' for staff who have not undertaken mandatory training. This includes automated notification of managers if a course is not completed. A separate version of this training is available in an online format for any staff or volunteers who do not have access to the Thinqi system. For service areas that deal with a large amount of personal data, bespoke face-to-face training is also provided.

5.2 Breaches can be reported to the Information Governance team from internal or external sources and in any way. Breach reporting is encouraged of any kind so it can be evaluated whether they are serious or not. People are not expected to have the 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**			
	2022/23	**2023/24**	**2024/25**	**2025/26**
Chief Execs	3	1	1	n/a
Children & Young People	12	10	7	6
Enterprise (Communities & Place)	13	10	6	13
Customer, Culture & Wellbeing - Mon Life	4	1	6	1
Law & Governance	3	2	8	1
People, Performance & Partnerships	1	2	4	4
Resources	0	0	0	1
Schools *(own Data Controllers)*	*21*	*16*	*38**	*37**
Social Care, Health & Safeguarding	32	24	25	27
TOTAL	**89**	**66**	**95**	**93**

**School breach reports have increased over the past year/s due to the active involvement of the Information Governance team with school business administrators and Head Teachers. Awareness of breaches has been raised, and schools are actively recognising issues and reporting them to the team.*

Table ii - Type of data breach

	2022/2	2023/24	2024/25	2025/26
Cyber Security Issue	0	0	0	0
Email**	70	52	74	59
Paper Records	11	3	9	12
Laptop/other devices	0	0	0	1
Other*	8	11	12	21
TOTAL	**89**	**66**	**95**	**93**

* '*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 (63%) of all breaches in 2025/26. However, this percentage had dropped over the previous 12 months. This is being monitored, but it is likely to be a result of more information being held and shared via Sharepoint Online, rather than as attachments.*

Table iii - Number of Data Breaches reported to the ICO

	2022/23	2023/24	2024/25	2025/26
Corporate	2	1	1	1
Schools	0	0	1	2
TOTAL	**2**	**1**	**2**	**3**

5.4 For the reports sent to the ICO regarding personal Data Breaches in 2025/26, two did not result in any penalties or sanctions. A decision from the ICO regarding the other report is still awaited. When responding to a report that requires no further action from themselves, the ICO issue a 'checklist' to support learning and training of staff.

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

	2022/23	2023/24	2024/25	2025/26
Corporate	19	31	27	29
Schools	1	3	4	7
TOTAL	**20**	**34**	**31**	**36**

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 have 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,' are tracked and are used to enhance training and other awareness activities. Staff are also encouraged to reflect on their practice and procedures, which often instigate a change in processes to ensure a breach is not incurred in future. It is positive that these incidents are reported to the team, even if very minor.

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.

Table v - Number of External Organisation Breaches and Incidents

	2022/23	**2023/24**	**2024/25**	**2025/26**
Corporate	5	7	9	4
Schools	2	1	4	6
TOTAL	**7**	**8**	**13**	**10**

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. As well as the steady increase in Subject Access requests, the volume of enquiries for other information 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 2022/23 94 DSARs
Financial Year 2023/24 108 DSARs
Financial Year 2024/25 115 DSARs
Financial Year 2025/26 123 DSARs

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

Data Subject Access Requests	2022/23 Number	2023/24 Number	2024/25 Number	2025/26 Number
Children's Services	69	57	68	63
Adult Services	9	16	7	16
Mixed Children's and Adult Services	10	4	37	10
Whole Authority	6	31	3	34
TOTAL	**94**	**108**	**115**	**123**
No. of individual requestors above	*67*	*88*	*92*	*95*
No. of 'on time' replies (28 days)	*64%*	*65%*	*58%*	*60%*
No. of enquiries received concerning potential illegal activities eg, National Fraud organisations, Rent Smart Wales, Home Office Immigration	***11***	***31***	***112***	***191***

Due to the increasing complexity and amount of requests received, the Customer Relations and Information Security & Technology teams are looking into ways to support managing and responding to requests. This includes discussions with other Local Authorities and the SRS regarding the use of software and AI to support the redaction process. However, DSARs will always require significant human input to ensure the security and integrity of highly sensitive personal data.

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**