ANNUAL REPORT 2024/25

Information Governance

Contents

1 Introduction

The Council processes a lot of sensitive information on behalf of the people in Plymouth who need to be confident that we protect that information appropriately.

Scrutiny from the public over how the Council processes their data is increasing, with an increase in members of the public complaining about any breach of their data both directly to the Council and to the Information Commissioner. Some of these complaints are resulting in claims for compensation, which will be covered in a section of this report.

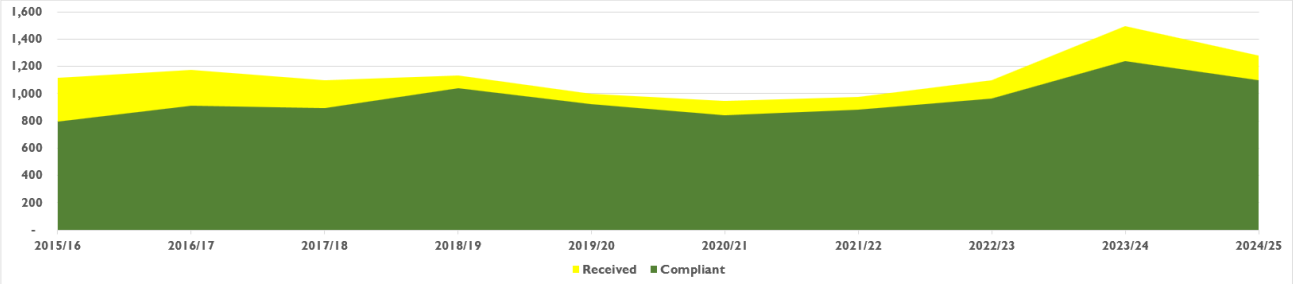
2 Information Access – Freedom of Information

Freedom of Information requests were lower than 2023/24, with a 14% decrease. This is due to the high volume of requests received last year regarding Armada Way. This year 1,281 requests were received, the highest amount recorded for a year, discounting the Armada Way requests.

The Council has experienced an increase in the percentage of requests completed within timescales, which is now 86% compared to 83% in 2023/24.

	Average	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25
Received	1,122	1,092	1,155	1,061	1,116	996	949	976	1,097	1,494	1,281
Compliant	990	922	1,033	963	1,042	923	839	883	961	1,238	1,097
Compliant %	89%	84%	89%	91%	93%	93%	88%	90%	88%	83%	86%
Non compliant	132	170	122	98	74	73	110	93	136	256	184
Non compliant %		16%	11%	9%	7%	7%	12%	10%	12%	17%	14%

Annual Increase	2 Year	5 year average	5 Yr Av comparison
86%	117%	1,102	116%



Below is a breakdown of requests by department for the last ten years, which shows which departments receive the most requests and the fluctuation in volumes. This year Strategic Planning and Infrastructure experienced the largest decrease, which is directly linked to the Armada Way requests last year. There were large increases for Community Connections, Finance and Public Health.

The table also shows the comparison for each department against a 5 year average, where the majority of departments are experiencing higher than average amount of requests.

Directorate	Department	Average	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25	% of total	Annual change	5 yr Av	% Ave
Adults, Health & Communities	Adult Social Care	76	83	88	73	76	73	75	65	73	74	77	6%	104%	72	107%
Adults, Health & Communities	Community Connections	90	55	82	105	79	78	62	87	106	108	137	11%	127%	88	155%
Childrens Services	Children, Young People and Families	74	93	70	44	55	88	62	78	56	112	80	6%	71%	79	101%
Childrens Services	Education, Participation and Skills	99	138	112	88	97	92	68	88	80	113	115	9%	102%	88	130%
Customer and Corporate Services	Customer Services	35	29	47	43	41	38	28	27	47	31	23	2%	74%	34	67%
Customer and Corporate Services	Digital and Customer Experience	20	3	4	11	33	25	23	36	25	27	15	1%	56%	27	55%
Customer and Corporate Services	HROD	45	35	55	70	72	12	38	30	26	67	48	4%	72%	35	139%
Executive Office	Executive Office	29	11	17	17	13	24	24	22	60	73	30	2%	41%	41	74%
Executive Office	Legal Services	11	11	19	10	4	5	6	13	3	21	22	2%	105%	10	229%
Finance	Finance	128	203	207	164	126	104	109	68	66	98	132	10%	135%	89	148%
ODPH	Public Health	30	37	24	23	34	19	13	18	39	30	58	5%	193%	24	244%
ODPH	Public Protection	89	85	108	87	111	125	100	82	72	56	65	5%	116%	87	75%
Other	Corporate	106	67	99	139	125	116	95	94	113	92	120	9%	130%	102	118%
Other	Debt	22	29	20	10	20	14	22	22	24	31	26	2%	84%	23	115%
Place	Economic Development	35	38	25	33	32	27	42	28	35	46	47	4%	102%	36	132%
Place	Strategic Planning and Infrastructure	109	47	55	53	67	69	69	104	138	360	130	10%	36%	148	88%
Place	Street Services	123	128	123	89	131	86	114	114	134	155	156	12%	101%	121	129%
Total		1,122	1,092	1,155	1,059	1,116	995	950	976	1,097	1,494	1,281		86%	1,102	116%

We have conducted a benchmarking exercise against other Councils in the region this year. On average, we receive less than most other Councils each year, and considerably less than the Unitary and county councils.

Organisation	5 yr Average	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25
Plymouth	1,112	1,230	1,092	1,155	1,061	1,116	996	949	976	1,097	1,494	1,157
Torbay	1,522	1,130	1,235	1,650	1,880	1,885	1,426	1,484	1,709	1,510	1,647	1,354
Devon	1,497	1,370	1,354	1,388	1,215	1,332	1,426	1,205	1,381	1,419	1,853	1,698
Cornwall	1,729							1,355	1,493	1,608	1,986	2,203
Exeter	745						774	735	685	802	839	635
Teignbridge	821	1,144	804	1,397	1,318	617	646	640	576	635	775	800
North Devon	747	618	536	700	817	873	760	596	731	743	825	828
Average		1,142	1,098	1,004	1,258	1,258	1,165	1,005	995	1,079	1,116	1,346	1,239

If we adjust the figures according to population size compared to Plymouth, we receive far less than all Councils apart from Cornwall.

Adjusted Figures

Organisation	Size Coeff	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25
Plymouth	1.00	1,230	1,092	1,155	1,061	1,116	996	949	976	1,097	1,494	1,157
Torbay	0.50	2,252	2,462	3,289	3,747	3,757	2,842	2,958	3,406	3,010	3,283	2,699
Devon	1.38	994	983	1,007	882	967	1,035	874	1,002	1,030	1,345	1,232
Cornwall	2.08	-	-	-	-	-	-	651	717	772	954	1,058
Exeter	0.45	-	-	-	-	-	1,729	1,642	1,530	1,791	1,874	1,418
Teignbridge	0.46	2,494	1,753	3,046	2,874	1,345	1,409	1,395	1,256	1,385	1,690	1,744
North Devon	0.34	1,825	1,582	2,067	2,412	2,577	2,244	1,760	2,158	2,194	2,436	2,445
Average		1,773	1,759	1,574	2,113	2,195	1,952	1,709	1,461	1,578	1,611	1,868	1,679

3 Information Access – Data Protection

The Council receives 18 different types of information request under the Data Protection Act. Subject Access Requests and Court Orders are the most complex of these request types, most of which are processed by the Information Governance team.

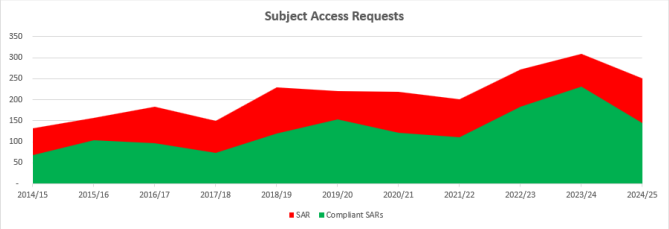
The table below shows the requests received by the whole Council, which overall is experiencing a slight decline in total requests.

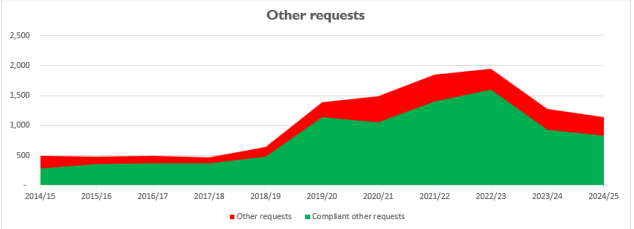
Section 3.1 provides details of the requests received by the Information Governance Team, which is experiencing an increase in total requests. This is due to changes in processes within some departments resulting in less requests being recorded corporately.

The figures for Subject Access Requests have been separated into two categories this year, standard requests which need to be completed within 30 days and more complex cases which can be extended to 90 days. The Council has determined that a case will be complex and need to be extended if the volume of pages needed to be processed exceeds the practical amount that can be processed within the 30 days.

The total number of Subject Access requests recorded by the Council has declined in the last year, with a 19% decrease in Subject Access Requests this financial year, a 8% decrease over two years.

Year	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25	Total	%	% 2Yr	% Av	5 Yr Av	Av/Mnth
SAR	132	156	183	150	229	220	218	201	272	309	250	2,889	81%	92%	102%	244	20
30 Day SAR	132	156	183	150	228	214	179	163	176	235	223	2,608	95%	127%	115%	193	16
30 Day Compliant SAR	68	104	96	74	118	149	108	99	138	187	127	1,597	68%	92%	93%	136	11
30 Day %	52%	67%	52%	49%	52%	70%	60%	61%	78%	80%	57%	61%	72%	73%	82%	70%	
90 Day SAR	-	-	-	-	1	6	39	38	96	74	27	281	36%	28%	53%	51	4
90 Day Compliant SAR	-	-	-	-	1	4	13	12	45	44	17	136	39%	38%	72%	24	2
90 Day %	0%	0%	0%	0%	100%	67%	33%	32%	47%	59%	63%	48%	106%	134%	132%	48%	
Compliant SARs	68	104	96	74	119	153	121	111	183	231	144	1,358	62%	79%	90%	160	13
SAR %	52%	67%	52%	49%	52%	70%	56%	55%	67%	75%	58%	47%	77%	104%	89%	64%	
Other requests	489	485	492	474	650	1,395	1,495	1,855	1,954	1,283	1,145	10,953	89%	59%	72%	1,596	133
Compliant other requests	279	359	366	369	482	1,138	1,056	1,400	1,595	932	835	8,223	90%	52%	68%	1,224	102
Other %	57%	74%	74%	78%	74%	82%	71%	75%	82%	73%	73%	75%	100%	97%			-
Total requests	621	641	675	624	879	1,615	1,713	2,056	2,226	1,592	1,395	13,283	88%	63%	76%	1,840	153
Total Compliant requests	347	463	462	443	601	1,291	1,177	1,511	1,778	1,163	979	9,581	84%	55%	71%	1,384	115
Total %	56%	72%	68%	71%	68%	80%	69%	73%	80%	73%	70%	72%					



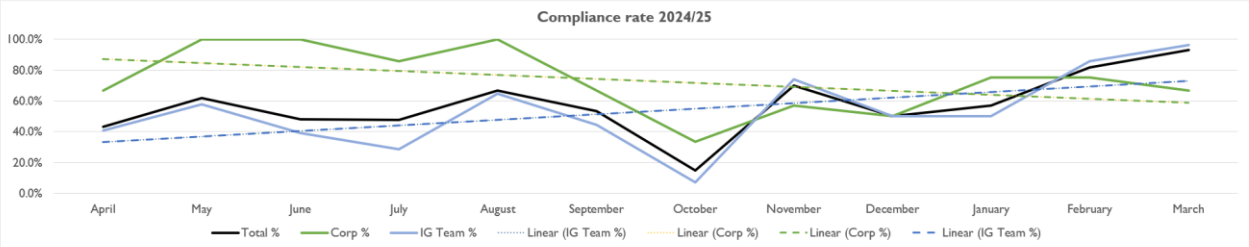


The compliance rate for standard requests is 57%, which is a decrease from last year of 23%, whereas the compliance rate for complex requests has risen from 59% to 63%. The reason for the decline for standard requests is due to a realignment of the definition of a complex request in line with ICO

guidance, resulting in far less requests meeting the criteria, which initially put additional demand on the Council, combined with a decrease in staff processing requests.

Additional capacity was put into the Information Governance Team in the Autumn, which has contributed to an improvement in compliance rates since then, which is shown in the table below, especially in the first three months of 2025, as the new staff have all undergone training and are reaching productivity levels from which we are realising the benefits.

Year	Month	Total	Total Compliant	Total %	Corp	Compliant	Corp %	IG Team	IG Team Compliant	IG Team %	Court Order	Other	30 Day SAR	30 Comp	30 Day %	Ext SAR	Ext Comp	90 Day %
2024/25	April	30	13	43.3%	3	2	66.7%	27	11	40.7%	18	76	18	8	44%	9	3	33.3%
2024/25	May	21	13	61.9%	2	2	100.0%	19	11	57.9%	31	101	16	10	63%	3	1	33.3%
2024/25	June	27	13	48.1%	4	4	100.0%	23	9	39.1%	24	107	23	9	39%	-	-	0.0%
2024/25	July	21	10	47.6%	7	6	85.7%	14	4	28.6%	34	82	14	4	29%	-	-	0.0%
2024/25	August	18	12	66.7%	1	1	100.0%	17	11	64.7%	12	76	17	11	65%	-	-	0.0%
2024/25	September	15	8	53.3%	6	4	66.7%	9	4	44.4%	32	87	9	4	44%	-	-	0.0%
2024/25	October	20	3	15.0%	6	2	33.3%	14	1	7.1%	24	80	14	1	7%	-	-	0.0%
2024/25	November	30	21	70.0%	7	4	57.1%	23	17	73.9%	45	121	23	17	74%	-	-	0.0%
2024/25	December	14	7	50.0%	8	4	50.0%	6	3	50.0%	27	109	4	3	75%	2	-	0.0%
2024/25	January	14	8	57.1%	4	3	75.0%	10	5	50.0%	25	96	7	2	29%	3	3	100.0%
2024/25	February	11	9	81.8%	4	3	75.0%	7	6	85.7%	34	91	5	4	80%	2	2	100.0%
2024/25	March	29	27	93.1%	3	2	66.7%	26	25	96.2%	36	119	18	17	94%	8	8	100.0%
Total		250	144	57.6%	55	37	67.3%	195	107	54.9%	342	1,145	168	90	54%	27	17	63.0%



The trend lines indicate the growing improvement in the Information Governance team, however also a declining trend for the rest of the Council as volumes have increased. This will be addressed by the proposed realignment of the Information request process which will accompany this report.

The table below shows the breakdown of SARs received by department, with the largest drop in requests being experienced by the Place directorate, which had 17 SARs in 2024/25 compared to 61 SARs in 2023/24.

Departmental SAR stats	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25	Total	%	% 2Yr	% Av	5 Yr Av	Av/Mnth
Childrens Services	-	-	-	-	-	-	-	2	-	-	-	2	0%	0%	0%	0	0
Corporate	-	1	-	3	10	5	3	10	7	7	8	34	114%	80%	125%	6	1
Councillors	-	-	-	-	-	-	-	-	-	-	-	-	0%	0%	0%	-	-
Customer and Corporate Services	2	6	6	1	11	29	11	6	6	8	13	105	163%	217%	108%	12	1
IG Team	98	101	107	106	128	124	165	145	208	205	195	1,391	95%	134%	115%	169	14
Executive Office	22	40	27	-	1	-	2	1	-	2	3	116	150%	300%	300%	1	0
External	-	-	1	-	-	-	-	-	-	-	-	1	0%	0%	0%	-	-
Finance	-	-	-	1	3	1	-	-	-	1	3	5	300%	0%	750%	0	0
ODPH	-	-	-	1	5	1	5	1	3	2	1	14	50%	100%	42%	2	0
People	7	2	20	25	13	8	4	5	9	23	10	106	43%	200%	102%	10	1
Place	3	6	22	13	58	52	28	31	39	61	17	284	28%	55%	40%	42	4
Total	132	156	183	150	229	220	218	201	272	309	250	2,058					

3.1 Data Protection requests processed by the Information Governance team

The majority of the Subject access requests are processed by the Information Governance team. These requests are the most complex requests as they mainly involve Social Care records. The Figures for the Information Governance team are below, which are showing a decrease of 5% in Subject access requests for this financial year, however this is 15% higher than the 5 year average.

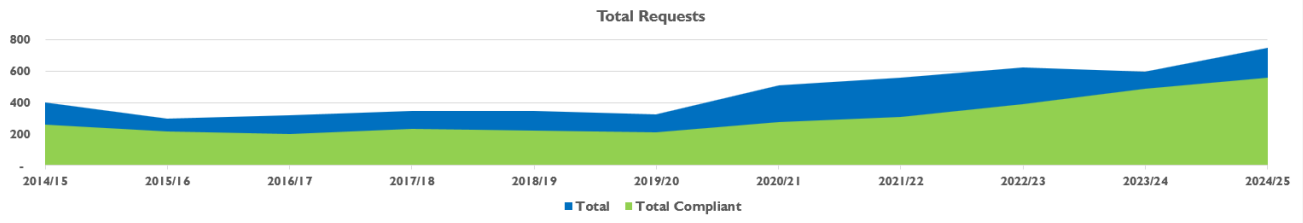
This figure varies from the requests recorded for the whole council as the Information Governance Team only processes as subset of the total requests for the Council.

The Information Governance Team also processes the Court orders for Social care records, which experienced an increase due to family breakdowns caused by lockdown. This figure decreased over

the last two years, however has increased by 89% during 2024/25, resulting in 336 court orders being processed, the highest amount recorded to date.

Total requests for the Information Governance Team increased by 25% for the year.

Type	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25	Prediction	%	2 yr %	% of Av	5yr Av	Av/Mnth
SAR	98	101	107	106	128	124	165	145	208	205	195	195	95%	94%	115%	169	14
30 Day SAR	98	101	107	106	127	118	126	107	112	131	168	168	128%	150%	141%	119	
30 Day Completion	63%	72%	54%	55%	46%	59%	59%	54%	74%	84%	54%	54%	64%	72%	81%	66%	0
90 Day SAR	-	-	-	-	1	6	39	38	96	74	27	27	36%	28%	53%	51	4
90 Day Completion	0%	0%	0%	0%	100%	67%	33%	32%	47%	59%	63%	63%	106%	63%	106%	48%	
Total Compliant	62	73	58	58	59	74	87	70	128	154	107	107	69%	84%	104%	103	9
%	63%	72%	54%	55%	46%	60%	53%	48%	62%	75%	55%					59%	
Court Orders	59	38	44	52	28	54	132	272	216	178	336	336	189%	156%	197%	170	14
Court Orders Compliant	44	36	36	42	26	47	98	154	136	160	316	316	198%	232%	266%	119	10
%	75%	95%	82%	81%	93%	87%	74%	57%	63%	90%	94%					74%	
Other	241	157	170	190	191	144	211	143	202	214	216	216	101%	107%	118%	183	15
Other Compliant	154	104	105	133	137	89	91	83	123	173	137	137	79%	111%	123%	112	9
%	64%	66%	62%	70%	72%	62%	43%	58%	61%	81%	63%					61%	
Total	**398**	**296**	**321**	**348**	**347**	**322**	**508**	**560**	**626**	**597**	**747**	**747**	**125%**	**119%**	**143%**	**523**	**44**
Total Compliant	**260**	**213**	**199**	**233**	**222**	**210**	**276**	**307**	**387**	**487**	**560**	**560**	**115%**	**145%**	**7%**	**333**	**28**
%	**65%**	**72%**	**62%**	**67%**	**64%**	**65%**	**54%**	**55%**	**62%**	**82%**	**75%**					**64%**	**0**
Police Disclosures	163	257	231	162	207	259	246	236	178	260	207	207	80%	116%	88%	236	20
Compliant	59	200	203	149	160	161	79	73	43	66	102	102	155%	237%	121%	84	7
%	36%	78%	88%	92%	77%	62%	32%	31%	24%	25%	49%					35%	



This is the first year the number of cancelled requests have been identified, and applied retrospectively. These are requests made by Data Subjects for their own or other people's data, where they have not been able to supply identification or consent for the information they are requesting. Each of these requests require officer time to follow up on the request. The figures show that this type of request is increasing.

	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25
SAR Cancelled	15	11	15	28	38	47	36	56	65	94	103
% Cancelled	13%	10%	12%	21%	23%	27%	18%	28%	24%	31%	35%

4 ICO performance intervention

The work on the ICO audit action plan has progressed with many of the actions closed. Outstanding actions will continue to be tracked on the action plan, and a progress report was shared with the ICO in June 2025.

The Health Determinants Research Collaborative (HDRC) programme in ODPH has provided funding for a post to complete some of the key actions, which has been filled with work underway. Service Directors have been contacted with details of the initial plan, with engagement due to start shortly to gather information about all of the data we hold.

The action around identifying improvements for the Information Access service reflects the Corporate Management Team's request for similar improvements.

5 Information Commissioner's Office (ICO) Escalations

In total, 14 complaints have been received during 2024/25. The Council received 13 complaints from the ICO during 2023/24.

5.1 Freedom of Information / Environmental information Regulations

The Council received 9 complaints regarding Freedom of Information / Environmental information Regulation requests.

- The Council did not respond to a request from July 2023 regarding tenders for Electric Vehicle Charge points (IC-293913-C7Y0)
    - This was an administrative error and the response was sent
    - These types of errors will be reduced with greater centralisation of request management.
- Complaint that the Council withheld information concerning Devon Housing Commission meetings (IC-284465-B8P6)
    - The Council had provided the requested information before the complaint was received
    - The complaint was withdrawn
- Complaint that the Council did not provide still birth rates for areas of the city (IC-287912-C5Z6)
    - This was related to the Energy for Waste plant.
    - The ICO issued a decision notice agreeing that the Council did not hold this information, however found that the Council had responded outside of the statutory time scale.
- Complaint about the Councils response for an explanation about a previous FOI response (IC-289690-L1B0)
    - A response was sent to the ICO by the Head of Legal Services
    - No further correspondence has been received from the ICO.
- Complaint that the Council did not supply information regarding a school, and didn't answer a question which related to an explanation of the response (IC-289690-L1B0)
    - The ICO agreed that the Council did not hold the information and that the Council did not breach the FOIA.

Complaint that the Council withheld information regarding communications with the police regarding campaign group STRAW (IC-323841-R0Z6)

- The ICO is investigating
- Complaint that an internal review for a information requested regarding their strategic boards had not been responded to (IC-360086-S9W5)
    - The response was sent.
- Complaint that an internal review for information requested around redevelopment of Wilmott Gardens had not been completed (IC-370995-W1M4).
    - The response was sent.

5.2 Data Protection

There have been 5 complaints to the ICO regarding Data Protection.

- Sensitive SEN documents sent to the wrong parents (IC-307372-S6T7)
    - The ICO stated that it does appear that the council has infringed the DPA as it inappropriately disclosed personal data to a third party.

    - The ICO took no further action as measures had been put in place to prevent further occurrences.
- Subject Access Request was outside timescales (IC-329922-Q0Q1)
    - The Council was asked to respond to the SAR within 28 days, which it did.
- Livewell staff member inappropriately access and shared information from Social Care systems (IC-326854-N7J4)
    - The ICO passed the case over to their criminal investigations team, however they cancelled their investigation as the Police issues a caution under the Computer Misuse Act.

Complaint that the Council did not rectify data in a Local Authority Designated Officer report as requested (IC-333781-X8Z4).
The ICO agreed that the Council did not infringe Data Protection obligations by not rectifying the data.
Complaint that the Council had not responded to a Subject Access Request by an ex-employee, (IC-349188-M7Z6)

- The Council has been asked to respond to the request.

5.3 First-Tier Tribunal escalations

A new first tier tribunal escalation was received in Q3 of 2024/25. These are cases where the complainant is challenging a decision notice issued by the ICO. The latest case is:

- The Council received an FoI requesting an explanation of why a request was responded to on the final day of the timescale and described as an operational issue.
    - The ICO decided that the Council would not have this information, and this decision is being challenged.

There are two other ongoing first tier tribunal cases.

- The Council received a request asking about payment history for a specific grave plot.
    - The Council is confident that all information has been supplied, which the ICO supported.
- The Council received a request for the audit report for the operator of the Energy for Waste plant, MVV.

The Council supplied the copy of the report that it had been provided with, which was only available in the German language as MVV is a German company.
The ICO agreed that the Council did not have an English language version to supply.

6 Data breach statistics

The Council has adopted an approach to managing data breaches where more events are recorded than necessary in order to implement lessons from low impact events in order to reduce the risk of breaches that meet the ICO reporting requirements. Therefore the figures are not published as this would provide a distorted view of the actual picture.

The number of breaches reported for 2024/25 resulted in an increase compared to 2024/25 of 25%. The number of breaches had decreased annually since the Data Protection Act was updated in 2018, however this year reverses that trend.

6.1 Data breach Types

The highest number of breaches this year have been electronic disclosures of information, both sensitive and non-sensitive with the latter increasing by 54%. Sensitive data breaches have a much higher impact on the data subject and a higher risk to the Council of further action from the ICO.

In most of the cases, the department took the appropriate actions to recover any disclosed information, reducing any impact on those affected, and applied appropriate mitigation. This is being done in a very timely manner, and will assist in reducing any referrals to the ICO.

6.2 Breach causes

Human error remains the largest overall cause, however it has increased in 2024/25 to 88%, compared to 2023/25 where 82% of all breaches were caused by human error within the Council.

- Email errors are the largest cause, with 53% of all breaches caused by an error using email, compared to 49% last year. This percentage was expected to decrease with increased use of more secure collaboration tools within Microsoft 365.
- Greater staff education of the use of the new tools will be needed to reduce the risk of breaches, especially as attaching the wrong attachment is the largest cause of breaches. The Microsoft tools we have reduce the need for sending attachments, as the document can be shared with recipients, removing the ability of unauthorised people opening the file.

6.4 Key lessons to reduce breaches

A number of key lessons have been shared with staff as a result of the breaches that have occurred this year. These are:

- If sending emails internally or to federated partners, utilise Microsoft 365 tools to share documents rather than send as attachments
    - This will allow access to the file to be limited to specific people
    - It will prevent access to the file if the email is forwarded onto others
    - It will also allow greater collaboration on the document
- Only access information on systems that you are authorised to access as part of your job role
    - Staff have access to systems with a lot of sensitive data about our citizens, and it is essential that this is not accessed or shared without a specific business purpose.
- Always double-check all aspects of emails before sending.
    - Addresses, including those that have been auto filled.
    - Always delete previous messages in an email trail unless absolutely necessary.
        - Email trails can contain information that should not be shared.
    - Use the BCC function if you're sending emails to multiple external recipients.
        - Email addresses containing a person's name is personal data, and can result in large compensation payments.
    - Autofill should be cleared regularly.
    - Attachments - read before you send.
    - Think first before clicking "reply all".
        - Do all of the previous recipients need to see your reply?
- Only use Council approved systems for processing any Council data.
    - Services known as Shadow IT can easily be used to steal data or compromise Council infrastructure.
- Ensure you and your staff use all messaging services and systems appropriately.
    - Any data in our systems may be subject to disclosure to a data subject.
- Always check that the data you are entering is correct.

- Incorrect data can cause a breach with a major impact.

7 Compensation Claims

There have three claims for compensation this financial year, due to distress caused by data breaches. All of these were received in Q4.

They are still being processed, so no payments have been made. A decision from our insurers is expected in Q1 of 2025/26.

8 Lost devices

The Council has recorded 13 lost devices this year. 2 laptops and 11 mobile phones. It is believed that this figure is underreported as devices are not being reported lost using the correct channels.

Directorates	Mobile Devices	Laptops	Desktops	Tablet	Other		Total
Councillors	-	-	-	-	-		-
Customer and Corporate Services	-	-	-	-	-		-
Executive Office	-	2	-	-	-		2
External	1	-	-	-	-		1
Childrens Services	4	-	-	-	-		4
EPAS	1	-	-	-	-		1
Corporate	-	-	-	-	-		-
ODPH	-	-	-	-	-		-
People	-	-	-	-	-		-
Place	5	-	-	-	-		5
Finance	-	-	-	-	-		-
					-		
Total	11	2	-	-	-		13

We are working with delt to address the gap in reporting, however need staff to raise the appropriate breach report in Firmstep.

9 Records management

The centralised paper-record retrieval service has been running since February 2023 and since the start of 2023/24, has received 258 orders and processed 1,055 files.

With two full years now completed, it is possible to start making comparisons about how the service is being used and by which teams:

	2023-24	2024-25	% Change
Orders received	125	133	+6%
Total files processed (dispatched & returned)	534	521	-2%

Overwhelmingly, the main user of the service remains the Information Access Team, requesting social care files to complete subject access requests, followed by the Adoption and Fostering services:

Team	2023-24	2024-25	Annual Comparison	Total
Information Access Team	78	84	108%	162
Adoption	16	16	100%	32

Fostering	10	20	200%	30
Children's Social Care	6	1	17%	7
MASH	2	-	0%	2
Legal Services	12	7	58%	19
HR	1	1	100%	2
Economic Dev	-	2		2
Livewell	-	1		1
Corporate	-	1		1
Total orders	**125**	**133**	**106%**	**258**

It is worth noting that 27% of orders have resulted in no files being found. Properly concluding that no paper files are held (as opposed to the file being misplaced or lost) takes time to check both current and historical cataloguing and sometimes to physically check multiple boxes in the record store. This is work that previously would have been done by service teams, including having to travel to the old store locations, and is a clear benefit to the Council of both the centralised paper record store and retrieval service.

In the past year at the record store, we have:

Received and catalogued 500 new boxes of records from across the Council, including completing the movement of child social care, foster carer and personnel records to a larger and more suitable storage facility, meaning we now have all paper social care and foster carer records held in once place for the first time;
Moved legal records to a new location where they are being sorted by the service before being moved into the record store itself;

- Used the record store to house abandoned records the Council took possession of following the closure of the Dewi Sant Care Home, ensuring that sensitive records relating to residents and staff will be kept safe, and if necessary available for inspection, until they can be destroyed;
- Recently started discussions with local GP surgeries with a view to storing some of their patient records, presenting an opportunity to generate income;
- Completed the construction of an office area within the record store, allowing staff and their visitors to view files on site.

In addition to the above, we are currently engaged in work to identify and catalogue all personnel records held at the store, at the end of which we will have for the first time an accurate picture of the files held, helping to facilitate requests for information and reducing the chance of loss.

Away from the record store, the Corporate Records Manager has been involved in discussions around the adoption of SharePoint as a replacement for the S Drive, although the project remains in its early stages.

10 Staff eLearning completions

The eLearning for Data Protection, and IT security have been merged into once course named Data Protection and Information Security @ the Council. 83.2% of staff have completed the course, which

is an increase from last year of 0.1%, however less staff have completed the course as total staff number of staff on our establishment have decreased slightly from 2,144 since last year.

Although the number of established staff has decreased, the number of licensed people using our systems has increased. Because people not listed on our establishment are not tracked in the staff training completion, this causes a risk in increased breaches and other errors.

Directorate	Staff No	Data Protection & Information Security	Completion
Adults, Health & Communities	295	256	86.8%
Children's Services	531	416	78.3%
Customer and Corporate Services	492	440	89.4%
Executive Office	87	78	89.7%
Office Of The Director Of Public Health	92	80	87.0%
Place	608	481	79.1%
Total	**2,105**	**1,751**	**83.2%**

11 Data Protection and Information Security Policies

These policies will be reviewed in Q1 this year.

12 Cyber Security

Over the last 12 months we have been reminded of the cyber threat we face having seen our website targeted and taken offline by a series of denial of service attacks in the run up to Christmas and just after. Plymouth City Council was one of a number of UK local authorities who were targeted by a group of pro-Russian cyber criminals whose aim seemed to be to create disruption and generate some publicity. The first wave of these attacks resulted in our website being briefly taken offline and the news and search features disabled whilst the attack was underway (over a period of around 24 hours). After that we worked to implement cyber defences as recommended by the National Cyber Security Centre. These were in place around a month after the first attack, since then despite being targeted by the same group we have had no disruption to service for our customers.

In May this year we will have been using KnowBe4 for 12 months. KnowBe4 provides bite sized training for all staff each month and also confirm the effectiveness of our "human firewall" with test phishing attempts. KnowBe4 evaluates training uptake and the identification rates of test phishing messages each month to give us a risk score. Over the course of the last 10 months PCC's assessed risk score has dropped by nearly 10%. We should be pleased with the progress we have made and continue to promote to all staff the requirement to complete training and be alert to the threat from phishing.

Cyber assessments conducted by the Council, Delt and external 3rd parties have helped us identify our key risks and we hold a monthly Cyber Board to oversee actions to mitigate these. Over the course of the next 6 months Delt will be implementing new software to further strengthen a couple of key areas – asset management (knowing where our equipment is and whether it is secure) and user management (ensuring the access rights for joiners, movers and leavers reflect the requirements of their role/employment status). These investments will provide more visibility across our IT estate, helping to counter the threats we face. They also follow on from the work Delt have done in the last 6 months to automate much of the patching of our IT estate. This is vital work, as unpatched software can be exploited by cyber attackers. Investments in this area are keeping us compliant with

best practise. Delt and PCC are committed to ongoing investment in cyber security, responding to new and emerging risk and threat intelligence.

In terms of risk management, PCC recognisesthe importance of maintaining a robust cyber security posture to protect our information assets, systems, and services. Our position is to hold a low risk appetite for cyber security threats, ensuring that we minimize potential risks to the greatest extent possible while maintaining operational effectiveness. Our risk register will reflect this position.

We are committed to the following principles:

Risk Avoidance: We prioritise avoiding risks that could compromise the confidentiality, integrity, and availability of our information assets. This includes implementing stringent security measures and controls to prevent unauthorized access, data breaches, and other cyber threats.

Risk Mitigation: We actively seek to mitigate risks through continuous monitoring, regular assessments, and timely updates to our security protocols. We invest in advanced technologies and training to enhance our cyber resilience and reduce vulnerabilities.

Compliance: We adhere to all relevant legal, regulatory, and industry standards to ensure our cyber security practices are aligned with best practices. This includes compliance with the General Data Protection Regulation (GDPR), the National Cyber Security Centre (NCSC) guidelines, and other applicable frameworks.

Incident Response: We maintain a comprehensive incident response plan to swiftly address any cyber security incidents. Our goal is to minimize the impact of such incidents and restore normal operations as quickly as possible.

Continuous Improvement: We are committed to continuously improving our cyber security posture by staying informed about emerging threats and adapting our strategies accordingly. We encourage a culture of security awareness and proactive risk management across all levels of our organization.

By holding a low risk appetite, we aim to safeguard our information assets and ensure the trust and confidence of our stakeholders. We will continue to invest in our cyber security capabilities to protect against evolving threats and maintain the highest standards of security.

13 Recommendations

Action	Progress	Next stage	Expected Completion
Key Messages to be distributed to staff	Communications are producing material to distribute to all staff	Communications published as part of the Comms planner	Q1 2025/26
Data Breach Training	Training is available now	Senior Leadership Team to contact Information Governance if they would like a session arranged It is best practise that all departments should have staff trained, with priority given to departments regularly dealing with highly sensitive data	Ongoing

Mandatory training courses recorded for all staff		Engage with HR to produce an action plan to record staff training for those not on our payroll.	
Mandatory training courses	HR have been contacted to determine actions taken for staff who do not complete training	Action plan to be developed to follow up with staff who have not completed mandatory training. Note: this point is wider than IG training.	Q1 2025/26
Information Lead Officers Group (ILOG)	Terms of reference and request for new members of the ILOG issued to SLT. Some nominees for ILOG have been received, however there are gaps	Under represented departments will be contacted again to nominate appropriate staff for ILOG	Q1 2025/26
KnowBe4 reminders	Message to SLT asking them to continue to promote training on KnowBe4 to staff in all services	Monitor training uptake levels and target teams with low uptake more specifically if required.	Q1 2025/26
Records of processing activity (ROPA)	Contractor has been appointed to gather all of the required information	All information required with be gathered with engagement from departments.	Q1 2025/26
Information Access Centralisation	Plan has been prepared	CMT to review plan and either approve or ammend.	Q1 2025/26

14 Summary

This year has seen additional demands with respect to Information Access, both in volume and complexity of requests. This will lead to a challenging year in 2025/26 where we need to ensure we have enough resources to manage all of the Information Requests and actions resulting from the ICO audit.

We are seeing an increase in data breaches, and there is a concerning increase in the use of Shadow IT services, which will need to be addressed in the coming year. We still need to ensure that staff are continually improving, and not repeating previous errors, and it is recommended that departments take up the offer of bespoke training.

Information Access improvements have been made in the final quarter of 2024/25, with compliance rates for Subject Access Requests increasing, compliance reporting being fine-tuned and progress being made to gather essential information required to understand the data the Council processes.

Further improvements are planned for the coming year which will see greater centralisation of information requests, which is expected to bring greater harmonisation in processes and enhanced responses.