Data Protection Annual Report 2023/24

Activity and Performance 2023/24 “At a Glance”

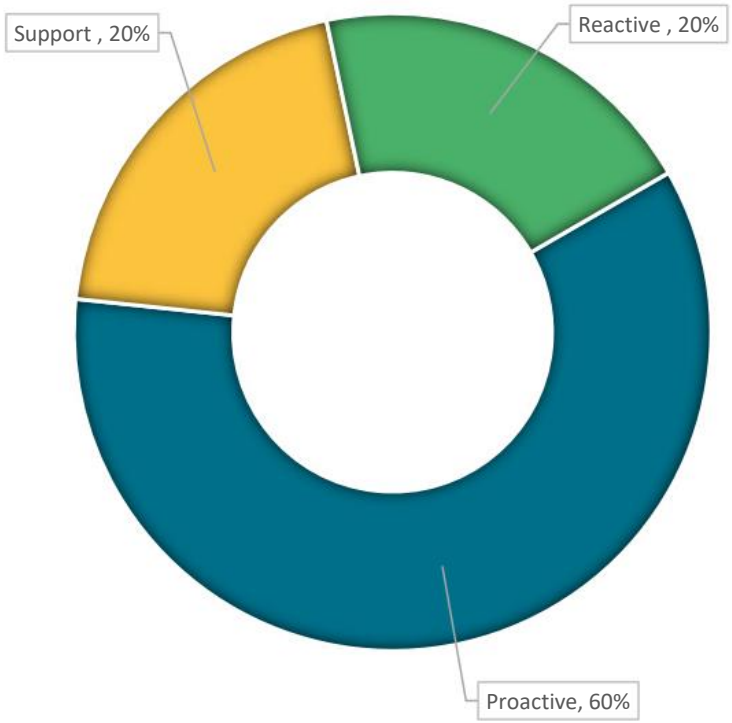
Compliance with Data Protection Legislation

Provision of independent strategic and operation-level advice, support and guidance on data protection, risk, and control processes.

Day to day management of the internal data protection function and ongoing quality control of data protection services.

The monitoring of internal compliance with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

A vast amount of proactive work and support has been undertaken with service areas to increase knowledge and awareness, resulting in a reduced amount of reactive work i.e. data breaches and ensuring the Council is compliant with Data Protection legislation.



Proactive	Data Protection advice covers a wide scope of work such as Data Protection Impact Assessments (DPIA), Data Sharing Agreements and general advice on topics such as privacy notices, releasing of information and how long information should be held for. Building knowledge and awareness through early intervention with projects to ensure data protection compliance. Other activities such as involvement in the tendering process and review of new contracts. Keeping up to date with changes to data protection legislation. Engagement with professional groups across the county identifying common trends and sharing best practice.
Support	Bespoke training on the importance of DPIAs and when and how to complete. Bespoke Customers Services and induction training for new officers. New Data Protection E-Learning modules rolled out to all officers and members.
Reactive	Data Protection breaches require the Data Protection team to act quickly in response, completing a risk assessment to ascertain whether the breach is a risk to the rights and freedoms of the data subject and whether it is to be reported to Information Commissioners Office (ICO) within 72 hours.

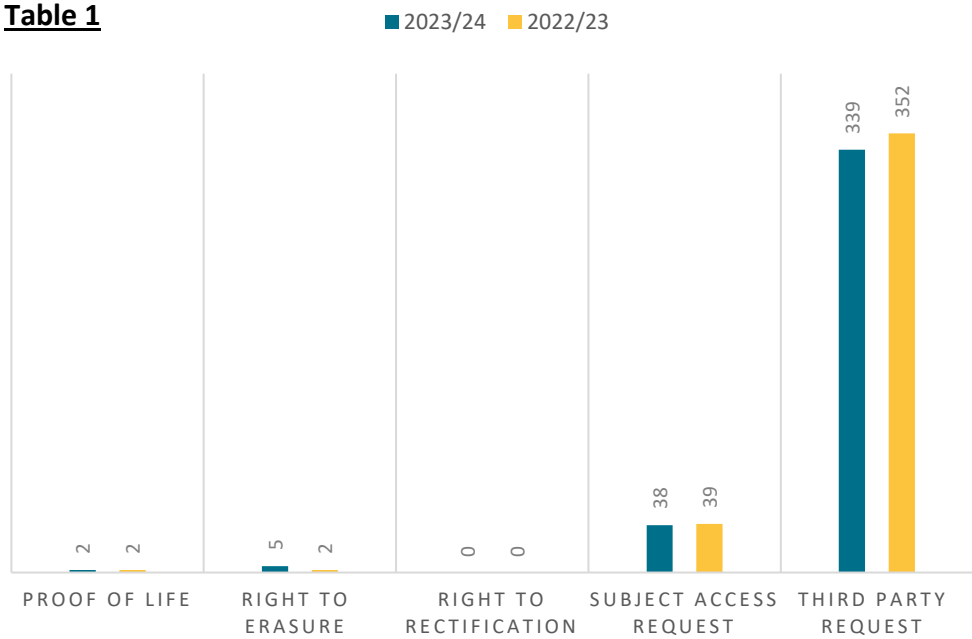
Data Protection Requests

A data subject has rights under data protection legislation, and can make requests including:

a) Right to erasure
b) Right to rectification
c) Right to access

Table 1, columns 1 to 4 show no real change year on year.

Table 1



The Data Protection team processed 39 data subject access requests in 2022/2023. Table 1, column 4 demonstrates a minimal decrease in the number of data subject access requests processed in 2023/2024. However, for the period 1 April 2023 to 31 March 2024 a total of 38 days was spent processing data subject access requests. For each data subject access request received, all relevant data requires collation and retrieval, reviewing for application of exemptions, and redaction of third-party information. Such requests can involve processing hundreds of documents.

The Data Protection team on average spent 1 day per data subject access request. However, the complexity and volume of data requested under the right of access has also increased. For example, one data subject access request for the period 1 April 2023 to 31 March 2024 took 3 days to complete. In conclusion every data subject access request is different resulting in challenges regarding resourcing this area as you can never predict the complexity and or volume of data that will be requested until the data subject access request comes in.

In addition to data subject requests, data protection legislation allows for third party requests. These are requests received by the Council for personal information relating to another individual, and can be received from other local authorities, the police, and utility companies.

The Data Protection team has seen a slight decrease in the number of third-party requests, table 1 column 5. However, the types of requests vary on a case-by-case basis and a valid lawful basis needs to be identified and considered om its own merit for each request.

Data Protection Reactive Work/Breaches

The Data Protection team investigates, and risk assesses all potential breaches to determine the likelihood that the data breach will affect the data subject. A data breach which results in a risk to the rights and freedoms of the data subject must be reported to the ICO within 72 hours of the Council becoming aware of the breach.

Table 2

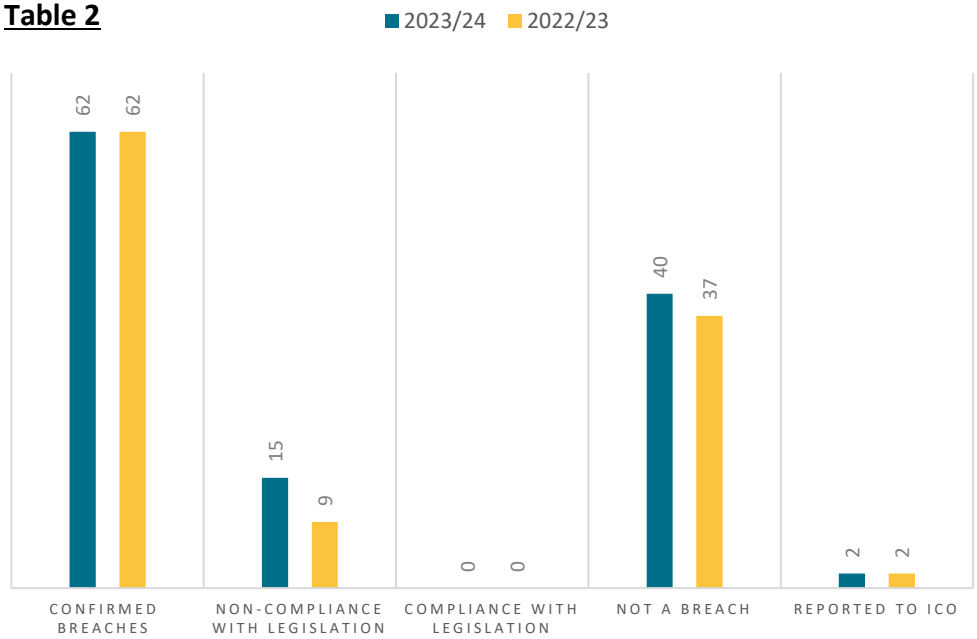


Table 2, column 1 demonstrates no increase in the number of confirmed breaches reported in 2023/2024. This could be due to:

a) A noticeable increase in approaches made by the Service Area's to the Data Protection team for general data protection advice and guidance generating increased knowledge and vigilance within service areas resulting in less errors/near misses by Officers.

The Data Protection team have reviewed all confirmed breaches for the period 1 April 2023 to 31 March 2024 and note the following trends:

a) Top three most common type of breaches 1) emails being sent to the incorrect recipient, 2) letters sent to incorrect addresses/recipients due to incorrect name or contact details updated (which includes accounts set up incorrectly) or multiple letters in one envelope and 3) improper publication of information on the Councils website. All the breaches following investigation have been due to human error, and none have been due to malicious intent. The majority of which following risk assessment have not required being reported to the ICO.

b) Most breaches are in the services areas that are customer facing across the Councils services, under time pressures to respond and have high interactions daily with customers which are time restricted. To mitigate some of the risk, bespoke training is delivered to the service areas that have high interactions daily with customers such as Housing, Customer Services, Planning etc. In addition, all new officers receive bespoke induction training as well as the e-learning modules.

Table 2, column 4 demonstrates a slight increase in the number of reported breaches that upon investigation were not a breach 2023/2024. This could be due to:

a) Proactive work and engagement with service areas creating more effective working relationships and rapport building resulting in Officers being more transparent.

Table 2, column 5 shows that two data breaches that were reported to the ICO by the Data Protection Officer (DPO) for the period 1 April 2023 to 31 March 2024 both of which were due to the incorrect release of personal data.

a) On both occasions the Council had demonstrated to the ICO that prompt action had been taken to mitigate the risk to the data subjects, and the ICO acknowledged the actions taken by the Council to resolve the breach at the time of reporting resulting in no further action by the ICO.

Table 2, column 2 shows a slight increase in the number of non-compliance with legislation. Non-compliance with legislation is where the Council has not adhered to one of the seven UK GDPR principles when processing personal data. Compliance with these principles is a fundamental building block for good Data Protection practice and key to the Councils compliance with the provisions of UK GDPR. These seven principles ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner,
2. Collected for a specified, explicit, and legitimate purpose,
3. Adequate, relevant, and limited to what is necessary,
4. Accurate and kept up to date,
5. Kept for no longer than is necessary,
6. Processed securely, and
7. Take accountability by demonstrating compliance with these principles.

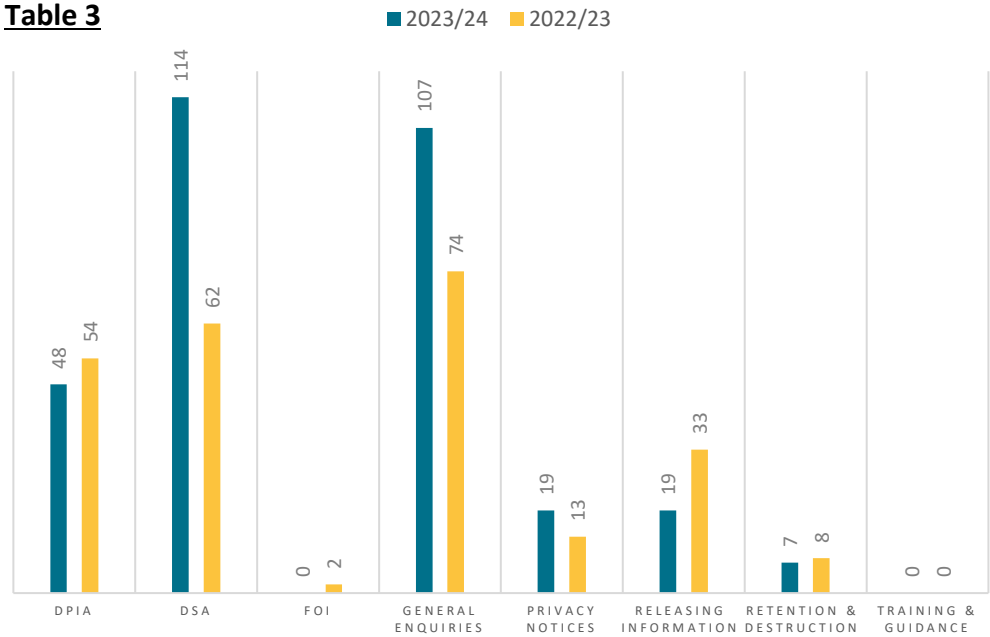
Table 2, column 3 shows no change year on year.

Data Protection Proactive Work, Support and Advice

The Data Protection legislation states that the Council is required to complete Data Protection Impact Assessments (DPIA), have data sharing agreements (DSA) and contracts in place, and are required to have privacy notices available to data subjects. The Data Protection team have been greatly involved in providing advice and guidance to service areas and assisting in completion of these documents.

The Data Protection team for the period 1 April 2023 to 31 March 2024 has delivered bespoke Data Protection training sessions to various service areas such as Planning, Housing Needs, Environmental Services and Customer Services. Focusing on varying topics for example lawful basis to process and publish information, how to handle Subject Access Request, records management, and email etiquette. Creating more effective working relationships and rapport building. This is evidenced in table 3, column 4 in the number of general enquiries received by the Data Protection team increasing significantly for the period 1 April 2023 to 31 March 2024.

Table 3



We continue to deliver further bespoke in-depth training as part of new Customer Services officer onboarding/enrolment process and bespoke training as part of all new officer's induction process in conjunction with the Data Protection and Data Security e-learning modules.

This financial year has seen an increase in not only the number of internal requests for advice, such as general enquiries (table 3, column 4) and DSAs (table 3, column 2), but also an increase in the complexity on the internal requests for advice for the period 1 April 2023 to 31 March 2024.

Table 2, column 2 shows a sharp increase in requests for advice regarding DSAs (inclusive of Contracts, Service Level Agreements and Memorandums of Understanding) this could be due to:

a) Proactive work and engagement with service areas specifically Procurement and Legal resulting in increasing knowledge of when and how to refer DSAs, Contracts etc to the Data Protection team.

Table 2, columns 1, 3, 5, 6, 7 and 8 show no real change year on year.

Resources

The Data Protection team consists of a Senior Information Governance Officer and an Information Governance Administrator the equivalent of 2 FTE. The Data Protection team successfully recruited the Information Governance Administrator mid 2022/2023.

As demonstrated in table 4 the total resources used by the Data Protection team in 2022/2023 for direct Data Protection activities was 403 working days. For the period 1 April 2023 to 31 March 2024 total resources used by the Data Protection team for direct Data Protection activities is 415 working days. This excludes time taken by the Data Protection Officer and Deputy Data Protection Officer.

This demonstrates that Data Protection team is currently resourced sufficiently.

Table 4