London Borough of Enfield

Report Title	2023-2024 Annual Data Protection Officer Report
Report to	General Purposes Committee
Date of Meeting	23 October 2024
Cabinet Member	Cllr Ergin Erbil, Leader of the Council
Directors	Terry Osborne, Director of Law & Governance
Report Author	Andrea Kilby, Head of Legal Practice and Compliance
Wards affected:	All
Classification:	Part I Public

Purpose of Report

1. The Annual Data Protection Officer Report 2023-2024 (**Annex 1**) summarises:

- The role of the Data Protection Officer (DPO)
- Council's Data Protection Update
- Schools' Data Protection Update

2. Findings from the recent self-assessment.

Recommendations

I. The committee is recommended to note the work completed by the Data Protection Officer during 2023-24, the findings of the recent self-assessment and the planned work for 2024-25.

Report Author: Andrea Kilby, Head of Legal Practice and Compliance.

Appendices
Annex 1*:* Data Protection Officer Annual Report 2023-24

Background Papers
None

Data Protection Officer Annual Report 2023-24

October 2024

Contents

Data Protection Officer Role

The UK GDPR requires all public authority data controllers to designate a Data Protection Officer (DPO). The primary role of the Council's DPO is to ensure that the London Borough of Enfield processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

The role of the DPO is to:

- monitor internal compliance with data protection legislation
- to inform and advise on data protection obligations
- to advise on and review Data Protection Impact Assessments (DPIAs)
- to provide risk-based advice to the Council and its schools
- to raise awareness of data protection issues
- to undertake and commission data protection audits
- to be a contact point for "data subjects" (whether that be the public or
- internal employees)
- to be the point of contact for the Information Commissioner's Office (ICO)
- To review contracts to ensure that they are data protection compliant

In fulfilling that role, a DPO must:

- act independently
- be an expert in data protection
- be adequately resourced to carry out the role

The designated DPO must be able to directly report to the highest management level, must not receive instructions regarding the exercising of statutory tasks, and shall not be penalised or dismissed for performing those tasks.

The Council must support the DPO in performing his tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations.

Since June 2024, Sharlene Morris (Certified GDPR Data Protection Practitioner) has been appointed as the designated DPO as required by Article 37 of the UK GDPR.

Council's Data Protection Update

Data protection queries and advice

One of the key tasks of the DPO is to inform and advise the Council and maintained schools about their obligations to comply with the UK GDPR and other data protection laws. This is a requirement under Article 39 of the UK GDPR.

The DPO receives a wide range of queries about data protection matters. This involves both providing advice, guidance and supporting various internal processes. Advice is provided about intricate aspects of the law supporting the organisation in applying data protection in practice. The DPO also assists with various internal data protection practices such as the review of privacy documentation, monitoring of Data Protection Impact Assessments and maintaining the Records of Processing Activities.

During 2023-24 advice has been provided on the following issues, amongst others:

- Data Sharing Agreements
- Data Processing Agreements
- The role of the Council as a Data Controller and its implications
- The role of external agencies as Data Processors and its implications
- Data protection due diligence in contracts
- The application of the data protection principles
- Understanding the lawful basis for processing personal data
- Data Protection Impact Assessments
- Data protection risks
- Disapplication of the data protection provisions (exemptions)
- Data protection breaches
- Individual rights requests (including processing police disclosure requests)

Data Protection Breaches

The London Borough of Enfield in its capacity as data controller, is custodian of the personal data of individuals to whom we provide support or services or who we employ or otherwise work with.

The DPO is primarily responsible for ensuring that the Council appropriately handles and manages their data. This not only enables the Council to effectively manage records that contain both personal and non-personal data but also assists to prevent security incidents, that may incur risks to the individuals (data subjects) and their personal data, leading to a data breach.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally or deliberately lost, destroyed, corrupted or disclosed; if someone accesses the data or

passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

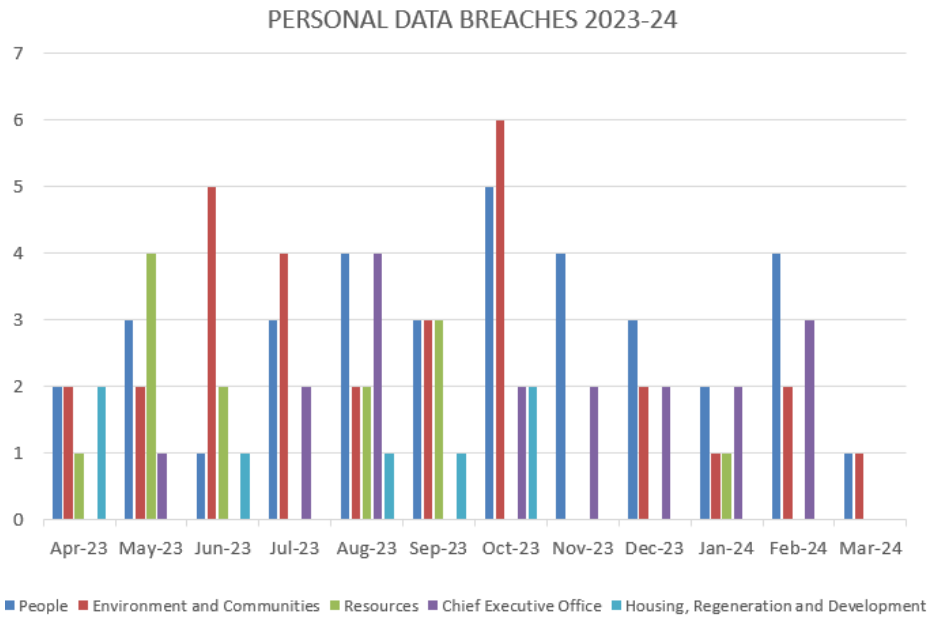
It is important for the Council to continue to pay sufficient regard to data protection and avoidance of data breaches, not only to ensure individuals' rights are upheld but also to avoid the potential imposition of enforcement action by the Information Commissioner's Office, (ICO); who potentially have the power to levy and enforce a maximum financial penalty, of £17,500,000 or up to 4% of annual global turnover, whichever is larger.

The Data protection team have implemented a robust Corporate and School data protection process, that has been involves the reporting of security incidents to the Council's Digital Security Service and Data Protection Team. Upon receipt of the notification, the incident will be investigated with the DPO advising if a personal data breach has occurred and, if so, promptly taking steps to address it, which could include reporting to the ICO, affected data subjects or any other relevant senior lead or regulatory body, when necessary.

The obligation to notify the Information Commissioners Office arises when a breach is deemed to be a 'high risk' to the rights and freedoms of affected individuals, causing potential harm or detriment to them. Breaches which need to be reported must be reported without undue delay, but not later than 72 hours after becoming aware of it.

The obligation to notify the affected data subject only arises when the breach is deemed to be a 'high risk' to the rights and freedoms of affected individuals. The affected data subject(s) should be informed without undue delay.

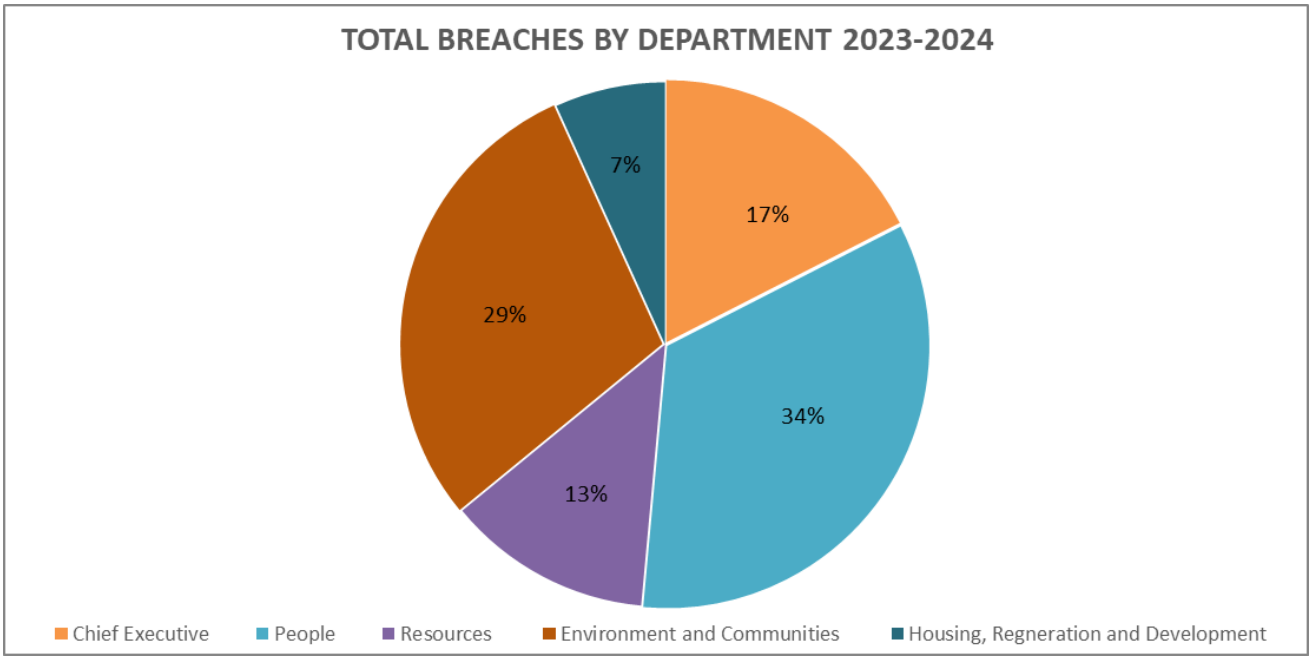
The DPO investigated a total of 106 personal data breaches between April 2023 and March 2024, this was an increase of 7 breaches in the year 2022-23. Below is a breakdown of all breaches by department.



	Apr 23	May 23	Jun 23	Jul 23	Aug 23	Sep 23	Oct 23	Nov 23	Dec 23	Jan 24	Feb 24	Mar 24	Total
People	2	3	1	3	4	3	5	4	3	2	4	1	35
Environ and Communities	2	2	5	4	2	3	6	0	2	1	2	1	30
Resources	1	4	2	0	2	3	0	0	0	1	0	0	13
Chief Executive	0	1	0	2	4	0	2	2	2	2	3	0	18
Housing, Regen and Development	2	0	1	0	1	1	2	0	0	0	0	0	7

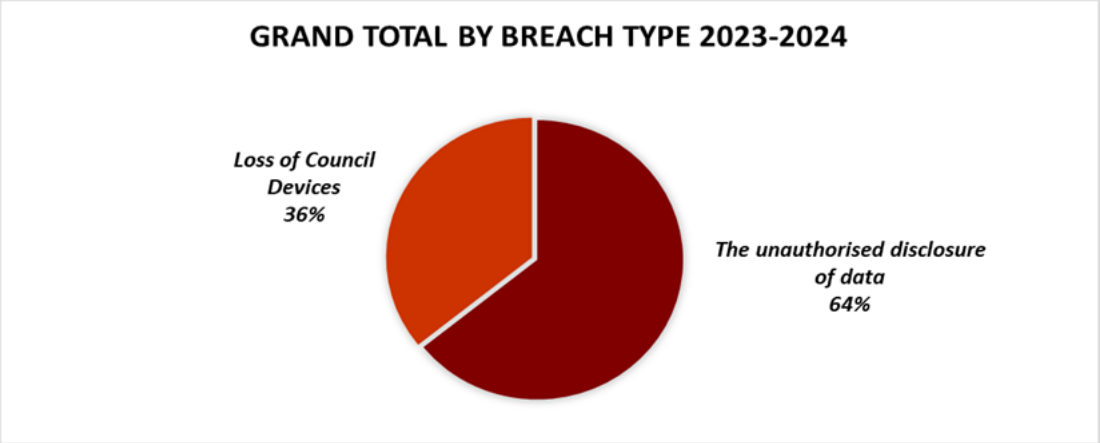
Currently the DPO has investigated a total of 62 personal data breaches between April 2024 and September 2025. Of those 62 personal data breaches a total of 8 have been reported to the ICO.

Of the reported data breaches 43% have occurred within the People Department. Whilst this figure is higher in comparison to the other Departments, the figure is proportionate as the Department processes personal data at a larger scale in comparison to the other departments.



These breaches can be divided into two broad categories:

- the unauthorised disclosure of data
- the loss of Council devices



The majority (64%) of the breaches have occurred due to the unauthorised disclosure of data. Of the 106 breaches reported 14 were considered to have met the threshold for reporting to the ICO. All incidents reported were thoroughly investigated and mitigation measures and longer-term actions to prevent reoccurrence were recommended by the DPO to the services.

It should be noted that there was an increase in the number of lost/stolen devices, 59 in 2023-24 compared to 38 in 2022-23. Investigation shows that during the year 2023-2024 there was a Digital Services project to recall old phones, which resulted in colleagues who had not used devices for an extended period of time and who could no longer find them reporting this in the lost/stolen Council device category.

Corporate Training

The training of staff and key stakeholders on their data protection responsibilities is one of the most important parts of any data protection compliance project or data protection structure in an organisation.

The mandatory e-learning training module (iLearn) for all staff on data protection was reviewed and updated during 2022-23. The data protection module has been amalgamated with the freedom of information and cyber security modules and renamed to Information Rights and Cyber Security. Between April 2023 and March 2024 all 233 new starters completed this training as part of their mandatory training and 823 colleagues completed the course as their required refresher training.

Information Commissioner's Office (ICO)

The DPO cooperates with the supervisory authority (ICO) with regards to complaints received about the Council's data protection practises. Between April 2023 and March 2024, the ICO published 2 decision notices. Decisions notices are the investigative outcomes following a complaint received by the ICO regarding our practices. Both decision notices related to complaints about information provided under FOI requests (processed under the Freedom of Information Act 2000) and both required no further action by the Council.

Self-Assessment Report

In April 2024 revised organisation reporting arrangements were implemented for the Data Protection Officer (DPO) and the Data Protection Advisor, as both posts moved from the Audit Team to the Legal Team, reporting to the Head of Legal Practice and Compliance and, by dotted line, to the Director and Law and Governance. This move allowed for continued independence of the DPO function whilst providing the ability to increase the data protection presence and resilience within the organisation through access to additional clerical support meaning that the DPO could focus on specific data protection tasks.

We have taken this opportunity to begin to conduct a full and thorough review of data protection within the organisation, relating to systems, processes, and culture. This review is being conducted against the ICO accountability framework, which allows us to self-assess across ten areas of review, namely:

1. Leadership and oversight
2. Policies and procedures
3. Training and awareness
4. Individual rights
5. Transparency
6. Record Of Processing Activity (ROPA) and lawful basis
7. Contracts and data sharing
8. Risks and Data Protection Impact Assessments (DPIAs)
9. Records Management
10. Breach response and monitor

We have chosen to focus initially on 4 areas which we believe will strengthen the current data protection processes and service provision. These areas are:

- 3. Training and Awareness
- 6. ROPA and lawful basis
- 8. Risks and DPIAs
- 10. Breach Responses and Monitor

Our progress on review and actions are set out below.

3. Training and Awareness

Training is mandatory and tracked, however it is generic to the whole organisation. For this reason, during 2024-25 we will once again review the mandatory training to ensure that it remains relevant and fresh, both for new starters and to those completing refresher training. For services, such as People Services, that handle large volumes of personal data we will review if additional mandatory training should be in place. Our aim is to have a proactive training programme that evolves across the course of the year to reflect events that take place and enable sharing best practice to teams across the Council based on experiences from others. We are

preparing a launch plan for replacement of the GDPR workbook which will cover training on completion of the DPIA, the legal requirements of a ROPA, IAR and retention schedule documentation. We will use available means of communication to raise awareness across the council of both exiting policies and procedures, for example how to report a data breach and new concepts such as the DPIA through channels such as Staff Matters emails and Intranet splash pages.

Where breaches occur the DPO within the investigation considers what training could prevent a repeat occurrence and where appropriate will schedule training as a future preventative measure before the breach investigation is signed off as completed. Since implementing this approach in September 2024, the DPO has delivered 3 training sessions.

6. Risks and DBIA and 8. ROPA and lawful basis

In the 2022-23 Data Protection Annual Report it was noted that since the inception of the General Data Protection Regulation in 2018, the Council has utilised a 'GDPR workbook' for two main purposes. The workbook, in an excel format, serves as a data register and links to the Record of Processing Activities (ROPA).

It is a legal requirement to maintain a record of processing activities. There are several specified areas where records must be maintained, such as the purposes of processing personal data, data sharing and retention.

The second purpose of the workbook is that it carries out a data protection impact assessment (DPIA). A DPIA is a process which helps identify and minimise the data protection risks of a project. It is required for processing that is likely to result in a high risk to individuals.

The previous format required all forms of new data processing activities to be recorded on the workbook whilst at the same time carrying out a DPIA. However, the requirement for a DPIA legally only exists in certain scenarios. In addition, the previous format does not allow for a pre-assessment for DPIAs of proposed projects, processing activity, technology prior to completion of a full DPIA form.

A new DPIA template was created and piloted in 2022-23 and following feedback amended in June 2024. This template includes a pre-assessment phase which allows business areas to assess whether a full DPIA is needed.

To replace the GDPR workbook in full alongside the DPIA we recommend and will implement the usage of the following documents in a stand-alone format;

- Record of Processing Activities (ROPA)
- Information Asset Register (IAR)
- Retention Schedule.

Having created the template formats for these requirements a project will be undertaken in the second half of the financial year 2024-25 to move the data from the existing workbooks to the new templates and will be launched in November 2024.

10. Breach Responses and Monitor

Following self-assessment against the accountability framework regards breach responses and monitor the following actions have been taken.

- The data breach reporting procedures have been updated with clear flow charts of the process. This has been agreed and shared with the relevant colleagues in Digital Services who support in directing data breaches logged through the Service Now system.

- The Data Breach Reporting Form has been updated to ensure that those reporting are prompted to include all the necessary information regards circumstances of the breach, such as,
  - How it was identified,
  - How it occurred,
  - What mitigating actions have been implemented and
  - What preventative measure could be put in place to prevent reoccurrence.

- The Data Protection Team investigates each breach in full and makes an assessment about whether the relevant threshold has been met to report to the ICO. The new form contains the outcome of that decision and reasonings.

- Tracking of data breaches has been updated and now includes details of remedial actions and preventative measures in place with who is accountable. Timescales are set for follow up actions from the DPO to review those measures and assess if they have been implemented and are delivering improved data protection measures within the service area.

Schools Data Protection Update

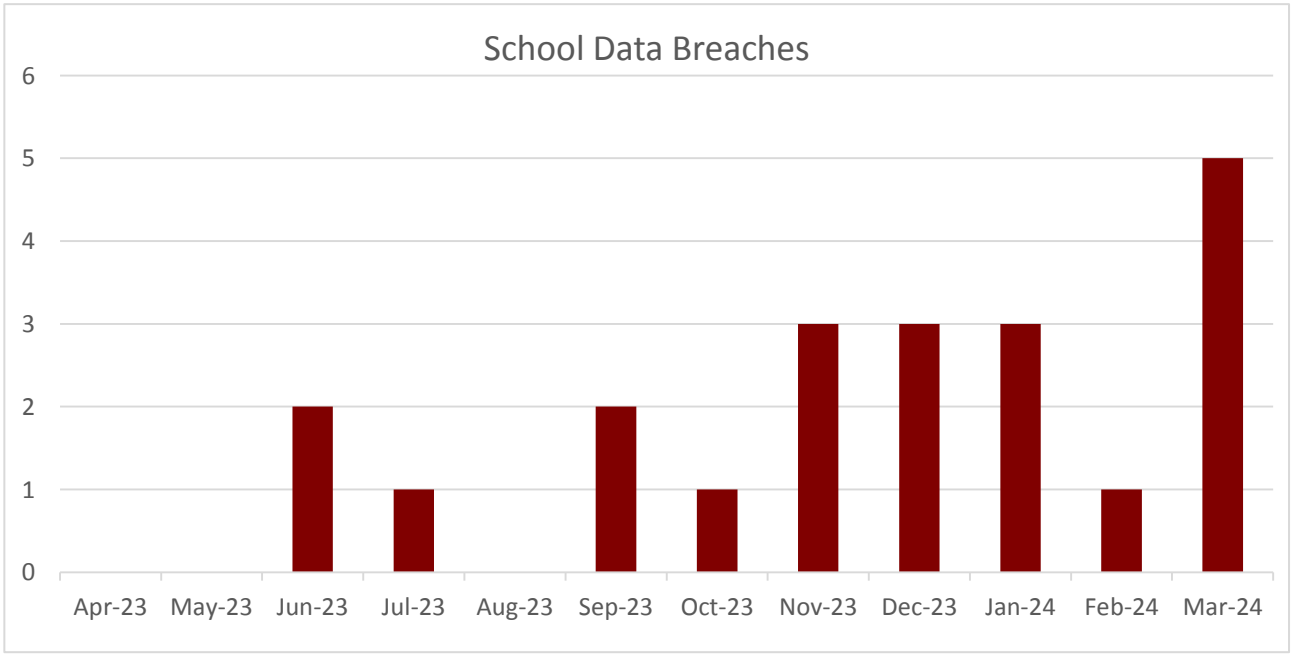
The Council provides a Data Protection Officer service to all its maintained schools via a de-delegated budget. Since June 2024 the DPO for the Council, Sharlene Morris, has filled this role. All maintained schools have agreed to sign up to the Council's DPO service for 2024-2025.

The DPO received a significant number of queries from senior stakeholders (Headteachers, Deputy Headteachers, Directors, and School Business Managers) within schools on a wide range of data protection issues. Most frequent queries are related to policies and data sharing. A common query received by the DPO is on the use of exemptions in relation to data subject requests. Advice has been provided during the year on this intricate part of the law and there is planned training for the 2024-25 academic year.

Data Protection Breaches

As part of the provision of the DPO service all schools report data breaches to the DPO and the same investigation process is undertaken for each breach.

Between April 2023 and March 2024 there were 22 school data breaches reported to the DPO. We are not aware of any incidents reported to the ICO. Below is a breakdown of the reports by month.



Schools Self-Assessment Report

In line with the approach for the Council the change of Data Protection Officer personnel is an opportunity to review the current services offered to schools. As part of the review, a UK GDPR checklist has been created for schools to complete their own self-assessment of the status of compliance assessing processes, procedures, security arrangements and culture. This will be launched in September 2024.These checklists will be returned to the DPO and will aid a desktop assessment of data protection procedures within school and inform required training for the academic year 2024-25.

In relation to the DPO completing the ICO self-assessment for the Council process and procedures where the outcome of the assessment identifies measures that would also prove beneficial for schools these measures will be introduced as part of the service offered by the DPO offered to schools. Example of this to date are listed below.

3. Training and Awareness

Upskilling our schools to be able to deal with most of the data protection and GDPR queries they have is a key strategy for the DPO in the academic year 2024-25. The UK GDPR checklist will identify skills gap which will inform further sessions to add to the already outlined schools training and awareness plan. Part of the awareness plan is to forge closer links with the School Business Managers, contributing regularly to the weekly update bulletins, making better use of the DPO Hub to share resources such as polices and templates and attendance at the School Business Manager forums.

6.0 Risks and DPIA and 8.0 ROPA and lawful basis

As per the identified action for the Council we will introduce the new Data Protection Impact Assessments (DPIA) and replace the GDPR workbooks with the standalone Record of Processing Activities (ROPA), Information Asset Register (IAR) and Retention Schedule. Having created the template formats for these requirements a project will launch in November 2024 to move the data from the existing workbooks to the new templates.

10. Breach Response and Monitor

- The Data Breach Reporting Form has been updated to ensure that those reporting are prompted to include all the necessary information regards circumstances of the breach, such as,

-How it was identified,

-How it occurred,

-What mitigating actions have been implemented and

-What preventative measure could be put in place to prevent reoccurrence.

- The Data Protection Team investigates each breach in full and makes an assessment if the relevant threshold has been met to report to the ICO. The new form contains the outcome of that decision and reasonings.

- Tracking of data breaches has been updated and now includes details of remedial actions and preventative measures in place for those who assume accountability. Timescales are set for follow-up from the DPO to review those measures and assess if they have been implemented and are delivering improved data protection measures within the service area.