London Borough of Enfield

Report Title	2022-2023 Annual Data Protection Officer Report
Report to	General Purposes Committee
Date of Meeting	28 June 2023
Cabinet Member	Cllr Tim Leaver, Cabinet Member for Finance and Procurement
Directors	Terry Osborne, Director of Law & Governance
Report Author	Gemma Young, Head of Internal Audit & Risk Management Gemma.Young@Enfield.gov.uk
Wards affected:	All
Classification:	Part I Public

Purpose of Report

1. The Annual Data Protection Officer Report 2022-2023 (**Annex 1**) summarises:

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

Recommendations

I. The committee is recommended to note the work completed by the Data Protection Officer during 2022-23 and the themes and outcomes arising from this work.

Report Author: Gemma Young
Head of Internal Audit & Risk Management
Gemma.Young@Enfield.gov.uk
Tel: 07900 168938

Appendices
Annex 1*:* Data Protection Officer Annual Report 2022-23

Background Papers
None

CE 22/045

Annex 1

Data Protection Officer Annual Report 2022-23

May 2023

Contents

Foreword

Data Protection Officer Role

Analysis on the Council's Data Protection Compliance

- Data Protection Queries and Advice
- Data Protection Breaches
- Data Protection Impact Assessments (DPIA)
- Corporate Training
- Information Commissioner's Office

Key Themes Identified

Schools Data Protection Update

- Compliance
- Data Protection Training
- Data Protection Breaches

Appendix 1 **Data Protection Officer – How role is discharged (as required by the UK GDPR)**

Foreword

There has been some good evidence of data protection compliance across the Council in general, however there are some areas for improvement which we will continue to support the Council to address in order to further improve the level of compliance.

An example of good practice is the widespread engagement of the Council's Data Protection Officer (DPO) in establishing the correct data protection role of other organisations when data is being shared with them. This is a crucial aspect of data protection law as identifying whether they are a data controller or processor has wide-ranging implications on the Council and its practices.

An area identified for improvement is the Council's Data Protection Impact Assessments (DPIA) process. DPIAs are a crucial process in ensuring the impact of data protection risks are controlled so that the rights and freedoms of individuals are not infringed upon. A new DPIA has been created and piloted. An awareness campaign for this new process will take place across the organisation in due course. This will be discussed in further detail below.

It is important for the Council to continue to pay sufficient regard to Data Protection not only to ensure individuals' rights are upheld but also due to the fact enhanced enforcement powers granted to the Information Commissioner's Office (ICO), including the power to levy a fine of £17,500,000 or up to 4% of annual global turnover, whichever is larger, can potentially be enforced.

As well as providing a Data Protection Officer (DPO) service to the Council itself, the London Borough of Enfield also provides a DPO service to all its maintained schools.

This report will address the work undertaken with both the Council and its maintained schools.

Please note that reference to the DPO in this report includes the data protection team.

Rezaur Choudhury
Data Protection Officer
LL.M, CIPP/E, CDPSE, BCS DPA, FOI and CISMP

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)

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 Data Protection Officer 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 April 2021, Rezaur Choudhury has been appointed the permanent designated DPO as required by Article 37 of the UK GDPR.

Analysis on the Council's Data Protection Compliance

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 on data protection matters. This involves both providing advice, guidance and supporting various internal processes. Advice is provided on 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.

Areas on which advice is being provided on include:

- Data Sharing Agreements
- Data Processing Agreements
- Understanding the role of the Council as a Data Controller and its implications
- Understanding the role of external agencies as Data Processors and its implications
- Application of the data protection principles
- Understanding the lawful bases for processing personal data
- Data Protection Impact Assessments
- Data protection risks
- Disapplication of the data protection provisions (exemptions)
- Data protection breaches

There has been a good level of engagement from different parts of the Council on various data protection issues. Advice is sought from the DPO on data processing at different stages. Whilst there has been good engagement from certain areas of the Council, DPO advice on data protection has at times been sought at the end/completion of projects. This has not enabled optimal achievement of one of the key data protection themes, data protection by design and default, which will be addressed in detail later.

Data Protection Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

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 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.

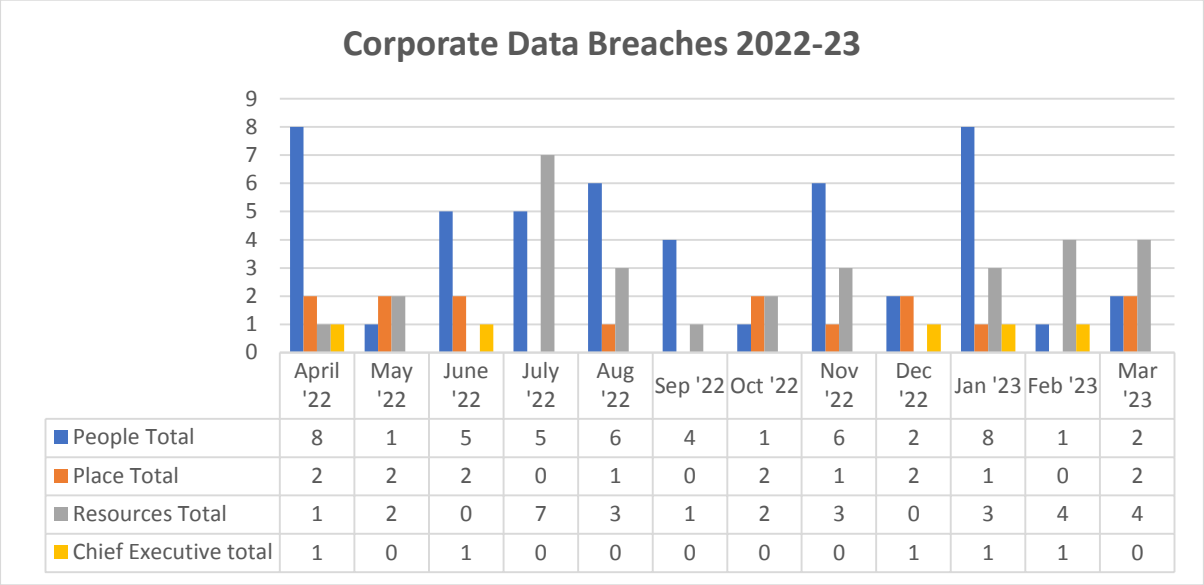
When a security incident is reported, the DPO advises if a personal data breach has occurred and, if so, promptly take steps to address it, which includes a report to the ICO and affected data subjects when necessary.

The obligation to notify the Commissioner arises when a breach is deemed to be a 'risk' to the rights and freedoms of affected individuals. 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.

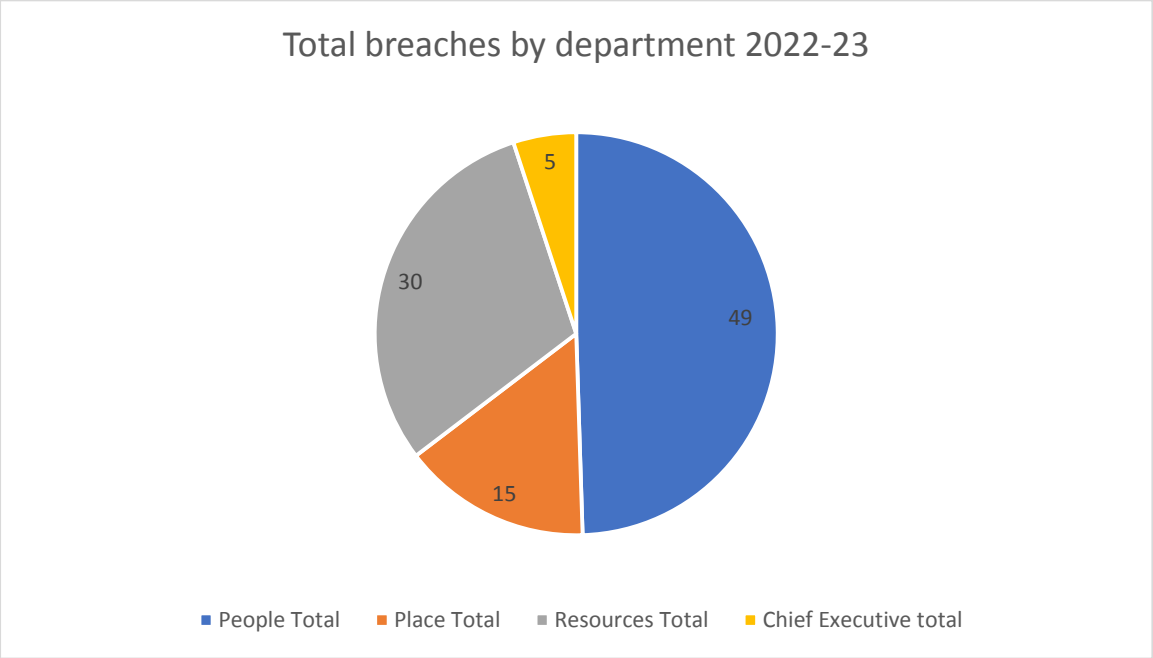
The DPO investigated a total of 99 corporate breaches between April 2022 and March 2023.

Below is a breakdown of all breaches by department.



	April '22	May '22	June '22	July '22	Aug '22	Sep '22	Oct '22	Nov '22	Dec '22	Jan '23	Feb '23	Mar '23
People Total	8	1	5	5	6	4	1	6	2	8	1	2
Place Total	2	2	2	0	1	0	2	1	2	1	0	2
Resources Total	1	2	0	7	3	1	2	3	0	3	4	4
Chief Executive total	1	0	1	0	0	0	0	0	1	1	1	0

Below is the total number of breaches by department.

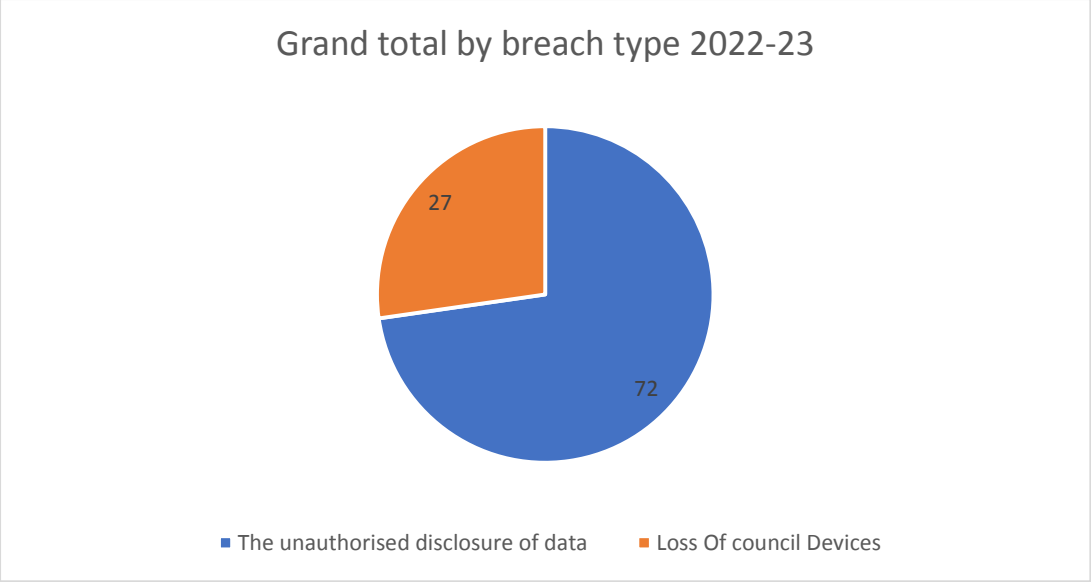


Approximately 49% of data breaches have occurred within the People Department. Whilst this figure is higher in comparison to the other Departments, the figure is proportionate as the Department processes personal data at a larger scale in comparison to the other departments.

These breaches can be divided into two broad categories:

- the unauthorised disclosure of data. This includes the accidental release of personal data and;
- the loss of Council devices

The majority (72%) of the breaches have occurred due to the former. Below is a breakdown of these breaches:



During this period, four data breaches met the threshold for reporting to the ICO. No further action was instructed by the ICO as the Council took reasonable efforts in mitigating the risks to the rights and freedoms of the affected data subjects.

Data Protection Impact Assessments (DPIA)

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.

A new DPIA template has been created and piloted. This template includes a pre-assessment phase which allows business areas to assess whether a full DPIA is needed. We are confident that the new format also allows business areas to fully assess necessity and proportionality within the context of a DPIA.

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 DPO has delivered a number of corporate training sessions.

- Data protection training which was provided to all elected members (June 2022 - September 2022). A total of 43 elected members attended these sessions

- Lunch and learn sessions on the following topics:

    - Data protection as a human right (November 2022)
    - History of data protection (January 2023)

The mandatory e-learning training module (iLearn) for all staff on data protection was reviewed and updated. The data protection module has now been amalgamated with the freedom of information and cyber security modules and renamed to Information Rights and Cyber Security.

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. These are complaints that the ICO receive from Enfield data subjects i.e residents and service user. Between April 2022 and March 2023 the DPO received 15 complaints via ICO regarding its practises.

Below is a breakdown of the complaints received from the ICO:

- 14 in relation to the Council's handling of data subject right requests. This includes right to access, right to rectification and right to erasure requests
- 1 in relation to a data breach

Key Themes Identified

The DPO has identified two key themes which if improved, will lead to an optimum data protection compliance overall for the organisation.

These key themes are:

- Implementation of data protection by design and default
- Data protection as a culture

Implementation of Data Protection by design and default

The UK GDPR requires that organisations adopt a data protection by design and default approach.

Data protection by design means that privacy and data protection issues are considered at the design phase of any system, service, product or process and then throughout the lifecycle.

Data protection by default requires organisations to ensure that only the data that is necessary to achieve the specific purpose is processed.

It is essential that the Council takes this approach with regards to its data processing. Adopting this theme will lead to an increase in compliance with the data protection framework. For example, the DPO's advice has been sought at the end of some project life cycles, this is not the most useful time to consult with the DPO as it does not allow for data protection by design and by default.

The DPO in collaboration with other key services will look to raise awareness across the organisation of this key theme, and training will also be provided on this matter.

As mentioned earlier, improvements have been made to the DPIA format. The DPIA is a key data protection by design requirement. It is envisaged that through using the enhanced DPIA template, the risks to the rights and freedoms of data subjects can be fully assessed and appropriate measures to manage risks can be implemented.

Data protection as a culture

Data protection should be viewed as a cultural issue. Data protection culture guides how things are done in an organisation in regard to data protection, with the aim of protecting the rights and freedoms of individual, ensuring compliance with the applicable rules and influencing employees' behaviour.

By changing day-to-day behaviours and fostering a cultural shift, the Council can proactively manage compliance and reduce the risk of data breaches. Whilst training has been delivered on data protection, there is a strong need to drive awareness across the Council and educating employees who handle and process personal data.

A communication plan is being developed by the DPO which will look at ways of driving awareness across the organisation. An increase in awareness will subsequently lead to an improved level of compliance.

Schools Data Protection Update

The Council provides a Data Protection Officer service to all its maintained schools. The DPO for the Council, Rezaur Choudhury, is also the DPO for all of the maintained schools. This service is a de-delegated service to all maintained Enfield schools. All maintained schools have agreed to sign up to the Council's DPO service for 2023-2024.

Compliance

There has been good engagement from Enfield Schools with the DPO. The schools in general seek the advice of the DPO before commencing with any data processing. A number of training sessions have been delivered to Enfield schools on data protection.

The DPO has received a significant number of queries from senior stakeholders (Headteachers, Deputy Headteachers and Directors) within schools on a wide range of data protection issues. A frequent query received by the DPO is on the use of exemptions in relation to data subject requests. Advice has been provided on this intricate part of the law and the engagement with the senior leadership teams within schools and the DPO has been positive.

Data Protection Training

Training sessions have been delivered to all Enfield Schools on various information rights topics.

Sessions have been delivered on the following topics:

- Data protection by design which was delivered in December 2022. There were in total 46 attendees over the course of three days with a total of 38 schools in attendance.

- Understanding Freedom of information and its exemptions (July 2022). There were 31 attendees and a total of 29 schools who attended.

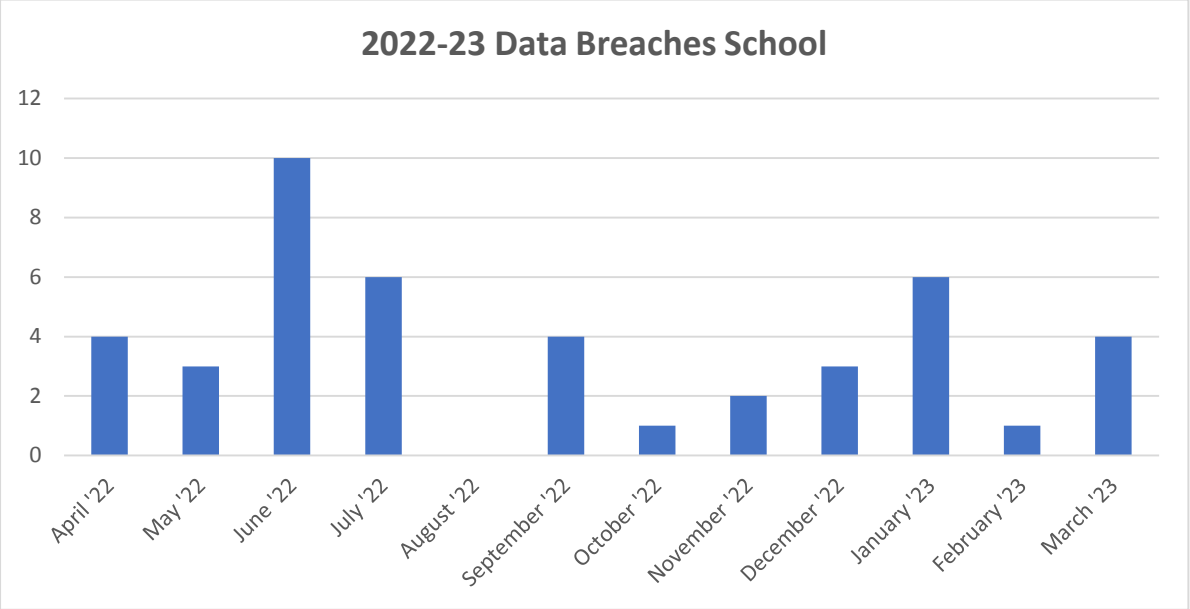
General data protection training to individual schools have also been delivered in person and via teams.

Following on from the accountability framework assessment completed with schools last year, the DPO identified training and awareness as an area for improvement. One of the concerns for schools was the lack of training available for all staff members. The DPO has prepared a data protection training presentation which has been disseminated to all schools. This presentation should be used by all staff members developing their understanding of data protection.

Data Protection Breaches

There were 44 school data breaches reported to the DPO. The DPO assessed nine of these to meet the threshold for reporting to the ICO. The ICO did not take further action with these breaches as the schools had taken reasonable steps to mitigate the risks.

44 of these breaches were in relation to the unauthorised disclosure of personal data. Below is a breakdown.



Appendix 1- Data Protection Officer – How the role is discharged (as required by the UK GDPR)

	Data Protection Officer/Organisation responsibilities	How it is practically discharged
	Position of the DPO	
1	The DPO must report directly to the highest level of management and is given the required independence to perform their tasks	Reports provided to assurance board periodically. The DPO also reports to the Head of Audit and Risk Management and is given the required independence to perform their tasks. Direct line to Chief Executive if required.
2	The DPO is involved, in a timely manner, in all issues relating to the protection of personal data	Member of Council's Information Governance Board.
3	The DPO is not penalised for performing their tasks	Contract of employment. Managed by Head of Internal Audit & Risk Management. Direct line to Chief Executive if required.
4	The DPO is not required to perform any other duties that result in a conflict of interest with their DPO duties	The DPO role is an independent role, no other duties are included.
5	The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39	Expert knowledge of data protection law has been demonstrated through the DPO holding a Master of Laws (LLM) degree in Information Rights Law and Practice and data protection practitioner level qualifications from the three main certifying bodies (IAPP, BCS, ISACA).
	Tasks of the DPO	
1	The DPO will inform and advise the organisation and its employees about the obligations to comply with the GDPR and other data protection laws	Key input/consultee into corporate guidance, training, policy development (advisory). Formal reports are provided to Assurance Board and General Purposes Committee.
2	The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, the data protection policies, awareness-raising, training and undertaking and commissioning audits	The DPO identifies any areas for improvements in compliance and brings this to the attention of the Assurance and/or Information Governance Boards.
3	The organisation will take account of the DPOs advice and the information the DPO provides on data protection obligations	Appropriate minutes/record will be taken regarding the advice / reports of the DPO and what action is taken.
4	The DPO will provide risk based advice, focussing on the higher risk areas of data processing activities, i.e. where special categories of data are involved	DPO consulted on DPIAs (see below) and through liaison arrangements regarding high risk areas.
5	The advice and input of the DPO	The DPIA process ensures the involvement of the

	will be sought when a Data Protection Impact Assessment (DPIA) is undertaken	DPO.
6	The DPO will also monitor the DPIA process	The DPO has access to all DPIAs and will undertake periodic checks to ensure consistency and appropriateness.
7	The DPO acts as a contact point for the ICO, and as such will co-operate with the ICO including during prior consultations under Article 36 (Prior Consultation) and will consult on any other matter	The relevant contact details for the DPO have been provided to the ICO.
8	The DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purpose of the processing	DPO considers and is consulted on the risks associated with processing activities to focus on higher risk areas
9	The DPO shall ensure that the organisation documents the reason why any advice given by the DPO is not followed	Appropriate minutes / records will be taken regarding the reasons why the advice of the DPO will not be followed.
	Accessibility of the DPO	
1	The DPO must be accessible as a point of contact for employees, individuals and the ICO	Within the confines of reasonable working arrangements, the DPO will be available and accessible. A 'deputy' DPO will be available should the DPO not be so due to annual leave or exceptional circumstances.
2	The contact details of the DPO are published and communicated to the ICO	The enfield.data.protection.officer@enfield.gov.uk email address is published in all appropriate places.
	Support to the DPO	
1	The DPO is provided adequate resources (sufficient time, financial, infrastructure and where appropriate staff) to enable them to meet their GDPR obligations and to maintain their expert level of knowledge	The DPO has an annual Performance Development Review to ensure sufficient focus is given to continuous training and development in data protection matters.
2	The DPO must be given appropriate access to personal data and processing activities	The DPO has unconstrained access to all personal data and processing activities in order to discharge his responsibilities and undertake independent and objective reviews.
3	The DPO be given appropriate access to other services within the organisations so that essential support, information and input can be received	The DPO has unconstrained access to all senior managers and services in order to discharge his responsibilities to provide support, advice, information, challenge and undertake independent and objective reviews.