London Borough of Enfield

General Purposes Committee

29 June 2022

Subject:	**2021-22 Annual Data Protection Officer Report**
Cabinet Member:	**Cllr Tim Leaver, Cabinet Member for Finance & Procurement**
Executive Director:	**Fay Hammond, Executive Director Resources**
Key Decision:	**N/A**

Purpose of Report

1. The Annual Data Protection Officer Audit Report (**Annex 1**) summarises:

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

Proposal

2. The General Purposes Committee is requested to note the 2021-22 Annual Data Protection Officer Report.

Reason for Proposal

3. Article 38 (3) of the United Kingdom General Data Protection Regulation (UK GDPR) requires that "…The data protection officer shall directly report to the highest management level of the controller…". This report fulfils this obligation.

Relevance to the Council's Plan

Good Homes in Well-Connected Neighbourhoods

4. An effective Data Protection Officer service helps to provide assurance over any risks that might adversely affect the delivery of good homes in well- connected neighbourhoods.

Safe, Healthy and Confident Communities

5. Compliance with data protection law and a strong enforcement of rights will result in safe, healthy, and confident communities.

An Economy that Works for Everyone

6. An effective Data Protection Officer service will help the Council achieve its objectives in building an economy that works for everyone.

Background

7. The tasks of the DPO are defined in the legislation.

   The Information Commissioner's Office summarises them as:

   - to inform and advise you and your employees about your obligations to comply with the UK GDPR and other data protection laws;
   - to monitor compliance with the UK GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
   - to advise on, and to monitor, data protection impact assessments;
   - to cooperate with the supervisory authority; and
   - to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

This report constitutes part of these tasks and is required by law.

Main Considerations for the Council

8. Under the UK GDPR, it is a duty for all public authorities to appoint a data protection officer (DPO).

9. The DPO assists the Council to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding data protection risks and act as a contact point for data subjects and the Information Commissioner's Office (ICO).

10. During 2021-22, the Council continued to improve its data protection practises. It is recognised that the Council needs to continue to build on its successes in this area and this is outlined and summarised in the 2021-22 Annual Data Protection Officer Report.

Safeguarding Implications

11. There are no safeguarding implications related to this report.

Public Health Implications

12. There are no Public Health implications related to this report.

Equalities Impact of the Proposal

13. Following completion of the Corporate Equalities Impact Assessment initial screening, this report does not have an Equalities impact**.**

Environmental and Climate Change Considerations

14. There are no environmental and climate change implications related to this report.

Risks that may arise if the proposed decision and related work is not taken

15. If the DPO does not report to the highest levels of the organisation, there is a risk that the Council will not fulfil its duties under UK GDPR.

Risks that may arise if the proposed decision is taken and actions that will be taken to manage these risks

16. N/A

Financial Implications

17. Failure to comply with data protection law could ultimately lead to significant fines from the supervisory authority. The Information Commissioner's Office can fine organisations up to £17.5 million or 4% of the annual turnover for non-compliance.

Legal Implications

18. Article 39 of the UK GDPR sets out the tasks of the DPO. The Council, not the DPO, is responsible for implementing appropriate technical and organisational measures to ensure that it is in compliance with the UK GDPR (Articles 24 and 28).

Workforce Implications

19. There are no specific workforce implications related to this report.

Property Implications

20. There are no specific property implications related to this report.

Other Implications

21. N/A

Options Considered

22. Given the requirement for the DPO to be able to directly report to the highest level of management, no other options were considered.

Conclusions

23. The General Purposes Committee is requested to note:

- the work completed by the Data Protection Officer during 2021-22 and the themes and outcomes arising from this work.

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

Date of report: 17 June 2022

Appendices

Annex 1: Annual Data Protection Officer Report

Background Papers

None

Annex 1

Data Protection Officer Annual Report 2021-22

June 2022

Table of Contents

Foreword

Since January 2021, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations, which have now been fully embedded into working practices across the Council.

Whilst there has been some good evidence of data protection compliance in general, there are some areas for improvement which the Council should address in order to further improve the level of compliance.

One of these areas is the Council's privacy notice. The privacy notice is a legal requirement and provides data subjects with privacy information at the time when personal data is collected. The current privacy notice is currently undergoing a review process to ensure full compliance with the data protection legal framework.

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 has also provided 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

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 of 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.

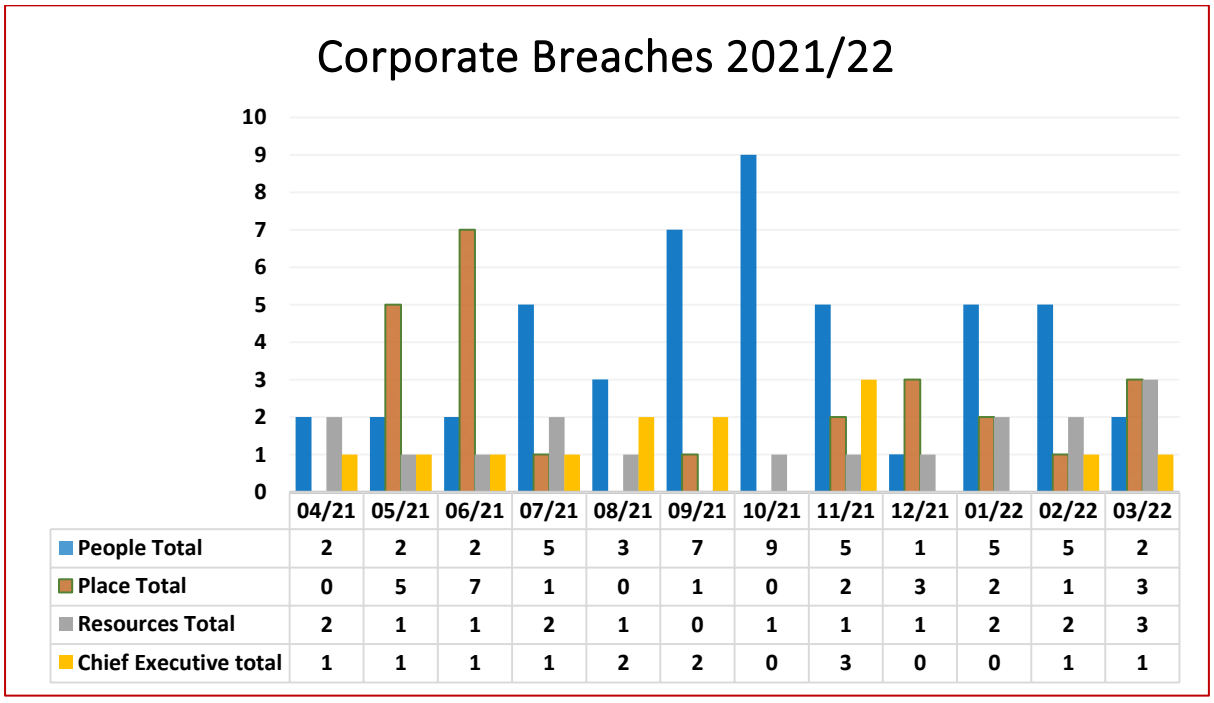
The obligation to notify the Commissioner arises when a breach is deemed to be a 'risk' to the rights and freedoms of affected individuals. Breaches which need to be reported must be reported without undue delay, but not later than 72 hours after becoming aware of it.

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 103 corporate breaches between April 2021 and March 2022.

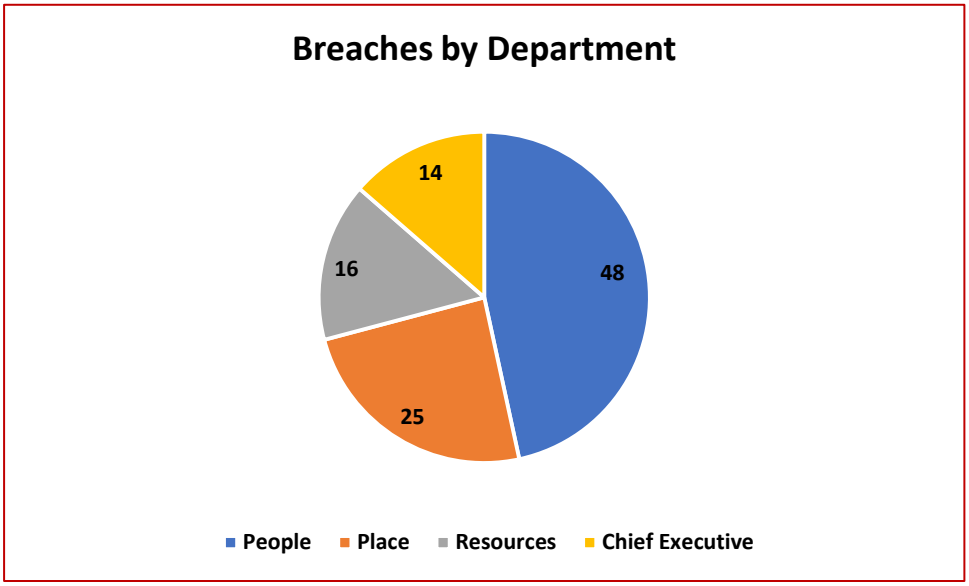
During this period, only two data breaches met the threshold for reporting to the ICO. No further action was instructed by the ICO as the Council took reasonable efforts in mitigating the risks to the rights and freedoms of the affected data subjects.

Below is a breakdown of all breaches by Department.



	04/21	05/21	06/21	07/21	08/21	09/21	10/21	11/21	12/21	01/22	02/22	03/22
People Total	2	2	2	5	3	7	9	5	1	5	5	2
Place Total	0	5	7	1	0	1	0	2	3	2	1	3
Resources Total	2	1	1	2	1	0	1	1	1	2	2	3
Chief Executive total	1	1	1	1	2	2	0	3	0	0	1	1

Below is the total number of breaches by Department:

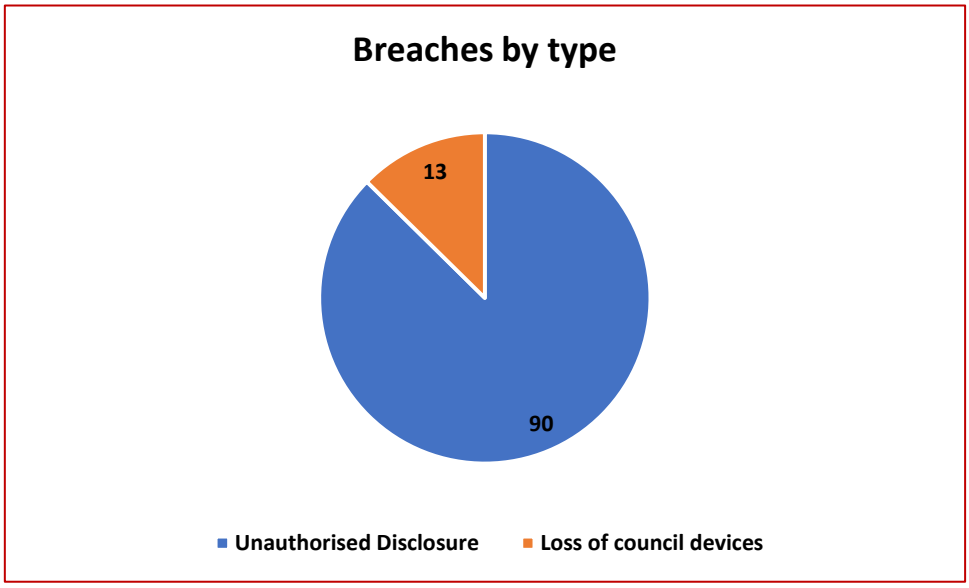


Approximately 45% of data breaches have occurred within the People Department. Whilst this figure is higher in comparison to the other Departments, the figure is proportionate as the Department processes personal data at a larger scale in comparison to the other Departments.

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 (87%) of the breaches have occurred due to the former. Below is a breakdown of these breaches:



Privacy Notices

A privacy notice is a document which must be provided to individuals to explain how their personal data is processed.

It has two aims:

- to promote transparency
- and to give individuals more control over the way their data is collected and used.

Transparency is a key principle of the UK GDPR, as it prevents organisations from processing personal data without data subjects' knowledge or approval.

When personal data is being collected directly from data subjects, it is a legal obligation to provide a privacy notice at the time of collection from the data subject.

The current privacy notice available on the internet, whilst it is informative, cannot comprehensively cover all the areas where personal data is being collected, due to the diverse nature of data processing across the Council. It is therefore important that all areas of the Council have privacy notices available at the point when personal data is collected.

Work has commenced on the Council's privacy notice and service areas, where required, will be supported in having an appropriate privacy notice in place. It is anticipated that this work will be completed by March 2023.

Nine privacy notices were created for different projects where personal data was being collected.

Data Protection Policy

The DPO has reviewed the existing data protection policy. A discrepancy was identified within the policy and the DPO has made an amendment to the definition of the personal data in relation to criminal offences.

The DPO will keep the policy under review for any future changes and will continue to promote compliance with the policy across the Council and its maintained schools.

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 the April 2021 and March 2022 the DPO received 10 complaints from the ICO regarding its practises.

Seven complaints related to the Council's handling of data subject right requests, two complaints related to data breaches and one challenge was received on the lawfulness of processing personal information.

Key Themes Identified

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

These key themes are:

- Implementation of data protection by design and default
- Transparency

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.

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.

Transparency

One of the key data protection principles is to process personal data in a 'lawful, fair and transparent manner'. The are some key transparency obligations upon the Council, such as the right to be informed. As mentioned previously, the Council will improve its current privacy notice in order to fully meet the UK GDPR's transparency requirement.

Revising the privacy notices will ensure that the Council is best-in-class in meeting its transparency obligations.

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.

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 response to these sessions has been positive with 75% of schools attending these sessions.

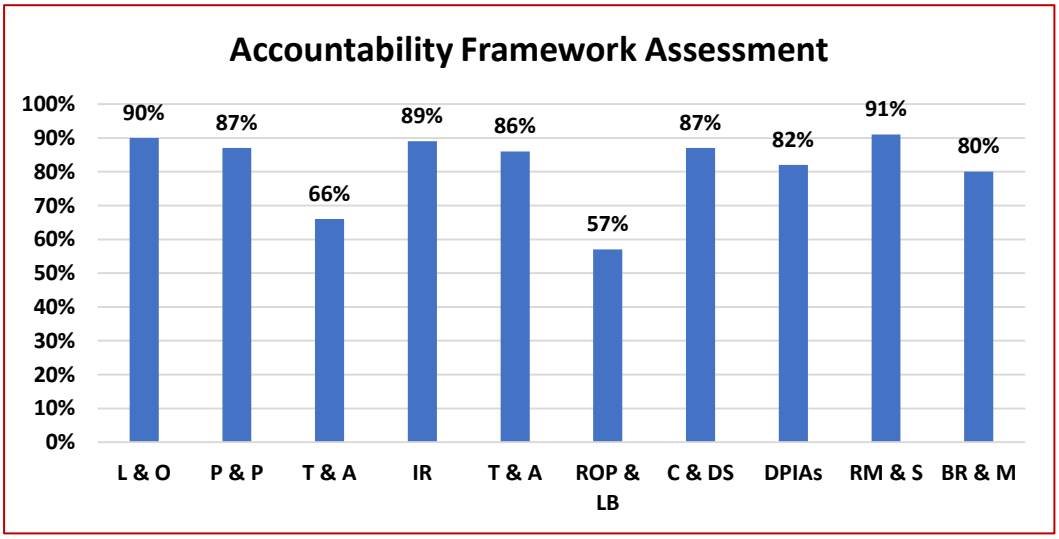
Accountability Framework

The DPO has supported Enfield Schools with the completion of the ICO accountability framework self-assessment. This assessment helps schools assess the extent to which they are currently meeting the ICO's expectations in relation to accountability.

The ten key areas which are assessed are as follows:

- Leadership and oversight (L & O)
- Policies and procedures (P & P)
- Training and awareness (T & A)
- Individuals' rights (IR)
- Transparency (T)
- Records of processing and lawful basis (ROP & LB)
- Contracts and data sharing (C & DS)
- Risks and data protection impact assessments (DPIAs)
- Records management and security (RM & S)
- Breach response and monitoring (BR & M)

13 schools participated in this assessment and overall the schools are meeting the ICO's expectations by 81%. Below is a breakdown of the results by area:



The DPO has been pleased to note that schools are keen to improve in the areas of training and awareness, records of processing and lawful basis. The DPO will create

an action plan to promote excellence in these areas and will work with the schools in improving their level of compliance.

Data Protection Breaches

There were a total of 29 school data breaches reported to the DPO. The DPO assessed three 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.

28 of these breaches were in relation to the unauthorised disclosure of personal data. One related to a lost device.

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.
	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 will be sought when a Data Protection Impact Assessment (DPIA) is undertaken	The DPIA process ensures the involvement of the 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	The relevant contact details for the DPO have been provided to the ICO.

	will consult on any other matter	
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.