ISLINGTON

Managing Individuals' Rights

A council-wide information policy
Version 4.0
December 2020

Contacts
If you need any further information about this document or any clarity about the contents of the document, please contact: The Information Governance Team (dp@islington.gov.uk).

Revision History

Date	Version	Reason for change	Author
28/1/15	0.1	First version – created from existing historical documents	Leila Ridley
30/1/15	1.0	Final version following comments from IG Team	Leila Ridley
20/8/15	2.0	Amended social media requests and removed reference to £10	Leila Ridley
01/03/18	3.0	Extensive revision to bring into line with new rights set out in GDPR	Leila Ridley
13/05/19	3.1	Updated to reflect legislation changes, changes to job titles and some change in responsibility	Brad Pearton
15/12/20	4.0	Annual review – minor changes to reflect Brexit/GDPR and new Case Management System	Brad Pearton

Table of contents

1. Purpose of this document

This procedure sets out the process for managing and responding to requests that fall under

'Individuals' Rights' as set out in chapter 3 of the UK General Data Protection Regulation (UKGDPR). These requests may be from individuals, or a representative acting on their behalf, this document details the agreed process for ensuring compliance with our legislative requirements.

This procedure applies to:

- Systems: All Information Systems in use in the council (both electronic and paper based). This includes information held on shared and personal drives and both group and individual email accounts.
- Staff: All employees, including contract and agency staff working for Islington Council.
- Information: All information, including opinions, relating to an individual.

2. Introduction

2.1 What is personal data?

The UKGDPR defines personal data as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller (the council) towards the individual, although in some limited circumstances exemptions will apply.

2.2 Who is the data controller?

The data controller is the person, or organisation that determines the purposes and means of the processing of personal data. Islington Council is the data controller for the personal data it processes.

2.3 The rights of data subjects

UKGDPR seeks to put data subjects back in control of their own data and increases both the right of access and sets out additional rights to ensure they can, to some extent, manage the information being processed by Data Controllers. A summary of the rights is as follows:

- The right to be informed
- The right of access (data subject access request)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

3. Managing the rights

This section will outline how the council will manage requests that fall under the individuals' rights and what information is required for the council to process a request. In all cases the rights must be responded to within one month, unless otherwise stated. The council is not able to charge for the requests, except in exceptional circumstances, this will be explained in more detail below.

An individual may submit their request verbally, via email, fax or letter. In addition to this it is also possible for a request to be received via social media. The request could be sent to any individual or team in the council, although we encourage individuals to submit their requests using the appropriate form and send this to foia@islington.gov.uk. The council must respond to all the requests it receives and therefore any requests received by staff or teams should be sent to foia@islington.gov.uk as soon as possible.

In respect of requests from the Department of Work and Pensions (DWP) for the personal data under joint control, the parties shall notify each other as soon as reasonably practicable. In the event the data subjects request further information from either party about how their personal data is being processed, the recipient party shall notify the other party and seek to agree on the content of the response to the data subject, within 7 working days of receipt of the request. Correspondence with DWP will be sent to hbsdsecurity.team@dwp.gov.uk

The Information Governance Team will ensure that the request is logged and acknowledged before allocating the request to the relevant department.

3.1 The right to be informed

The right to be informed obliges the council to be transparent in the way that it uses personal information and provide 'fair processing information', the council does this via its privacy notices. The information provided in the privacy notice is determined by whether or not the data was obtained directly from individuals. The table below outlines the information that the council must provide. The council have ensured that all privacy notices are:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓

Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible		✓

3.2 The right of access (data subject access request)

UKGDPR affords individuals with the right to obtain copies of information from a data controller, these are known as data subject access requests (DSAR). These requests do not need to be in a specific format however the council requests that these are in writing, the request does not have to state that it is a formal request for a DSAR for it to be a valid request. The council has an online form available for requests.

3.3 The right to rectification

UKGDPR enshrines the right for data subjects to have the right to instruct data controllers to rectify inaccurate personal data about themselves. This right takes into account the purpose of processing, but, in most cases, the data subject will be able to have incomplete data completed, which includes an option to provide supplementary information.

3.4 The right to erasure ('right to be forgotten')

This right gives the data subject the right to request that their personal data is deleted, this is not an absolute right. The council is only obliged to comply if one of the following grounds applies:

a) The personal data are no longer necessary in relation to the purposes for which they were collected of otherwise processed;
b) The data subject withdraws consent on which the processing is based and where no other legal basis applies.
c) The data subject objects to the processing, where it is carried out for the function of public task or the legitimate interests of the data controller, pending the verification whether the legitimate grounds of the council override that of the data subject. The data subject has the right to object to direct marketing at any time.

d) Personal data has been processed unlawfully.
e) Personal data must be erased for compliance with a legal obligation.
f) Personal data has been collected in relation to information society services where a child's consent has been obtained.

Whilst the council may not have to comply with a request for erasure, the council must respond to the request. Where the council is not obliged to comply we must, set out why we are unable to delete the information requested. If the council is able to comply, we will set out what information was held and confirm that is has been deleted

3.5 The right to restrict processing

This right gives the data subject the right to restrict the processing of their personal data, this is not an absolute right. The council is only obliged to comply if one of the following grounds applies:

a) The accuracy of the personal data is contested by the data subject for a period enabling the controller to verify the accuracy of the personal data;

b) The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.

c) The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

d) The data subject has objected to processing where it is carried out for the function of public task or the legitimate interests of the data controller, pending the verification whether the legitimate grounds of the controller override those of the data subject.

Whilst the council may not have to comply with a request to restrict processing, the council must respond to the request.

The council must explain why it does not have to comply with the request if that's the case. Where the council has restricted processing, it must tell the data subject the findings of its investigations and what it intends to do with the data and whether the processing will continue or cease

3.6 The right to data portability

This right is unlikely to apply to information that is processed by the council. However, this right gives data subjects the right to receive the personal data which they have provided to the council in a structured, commonly used and machine-readable format. The data subject will have the right to compel the data controller to transfer this information directly to another data controller where this is technically feasible. This right only applies where the data has been provided under consent and processing has been carried out by automated means.

3.7 The right to object

As with other rights, this is not an absolute right. Data subjects can only object to processing

where the council is processing information as part of a public task, or where it has legitimate grounds, including profiling, to do so. The council will have to comply with requests where we do not have legitimate grounds that override the interests, rights and freedoms of the data subject and it is not required for the establishment, exercise or defence of legal claims.

Data subjects can object to processing where it relates to direct marketing at any time. Where this applies, the council must cease the processing for direct marketing purposes.

The council must communicate its decision to the data subject, regardless of the decision. The council must clearly explain why it does not have to comply, where that is the case.

3.8 Rights in relation to automated decision making and profiling

This right entitles data subjects to request that decisions made about them are not based solely on automated processing, including profiling, which produces a legal effect concerning them, for example, someone's benefit entitlement. Should the council receive a complaint regarding such a decision, it will need to be revisited by 'human intervention'.

3.9 Verbal requests

The UKGDPR does not specify how to make a valid request, therefore it is possible to make a request verbally. If the council has received a verbal request the council will transcribe the request and ask the requester to confirm, in writing, that the council has correctly understood their request.

3.10 Requests submitted via social media

A request submitted via social media, for example, Twitter or Facebook, is a legitimate request and the council must make a response. The council believes that it is not always appropriate to respond to requests that relate to personal data over Twitter or Facebook and will request that the request is resubmitted via email or post. The council should direct the requester to the council's website for more information on how a request can be submitted, which will include the requirement to provide identification.

3.11 Entitlement to the information

When considering a request under the individuals' rights, the council must satisfy itself that the person making the request is entitled to do so.

a) Validating the identity of the requester

The council is entitled to request enough information to judge whether an individual is entitled to the information they are requesting or are entitled to make the request they are making. The council requests two pieces of identification and, in most cases the council will request copies of the following information from an individual before releasing information:

A copy of:

- Passport; or
- Driving licence; or
- Birth certificate

AND

A copy of:

- A recent bank statement (with full address) dated within the last 3 months; or
- A recent utility statement (with full address) dated within the last 3 months; or
- An Islington council tax number

The council will accept copies or scans which can be emailed to the council, sent via post, or brought in by the data subject on collection of the information.

Where the identity of the requester is known to you, for example there is an ongoing relationship to you, it may not be necessary to request identification.

b) Acceptable forms of identification

The following list sets out the forms of identity that the council will accept

Proof of name	**Proof of address**
Current signed passport	Utility bill (gas, electric, satellite television, landline phone bill) issued within the last three months
Original birth certificate (UK birth certificate issued within 12 months of the date of birth in full form including those issued by UK authorities overseas such as Embassies High Commissions and HM Forces)	Local authority council tax bill for the current council tax year
EEA member state identity card (which can also be used as evidence of address if it carries this)	Current UK driving licence (but only if not used for the name evidence)
Current UK or EEA photocard driving licence	Bank, Building Society or Credit Union statement or passbook dated within the last three months
Full old-style driving licence	Original mortgage statement from a recognised lender issued for the last full year
Photographic registration cards for self-employed individuals in the construction industry -CIS4	Solicitors letter within the last three months confirming recent house purchase or land registry confirmation of address
Benefit book or original notification letter from Benefits Agency	Council or housing association rent card or tenancy agreement for the current year
Firearms or shotgun certificate	Benefit book or original notification letter from Benefits Agency (but not if used as proof of name)
Residence permit issued by the Home Office to EEA nationals on sight of own country passport	HMRC self-assessment letters or tax demand dated within the current financial year
National identity card bearing a photograph of the applicant	Electoral Register entry
	NHS Medical card or letter of confirmation from GP's practice of registration with the surgery (not prescription)
Veterans Identification Card	

a) Requests made on behalf of others

The DPA/UKGDPR does not prevent an individual making a request on behalf of another, for example, a solicitor acting on behalf of their client. In these situations, the council must be satisfied that the third party making the request is acting on the authorisation of the data subject. In these situations, it is essential that the third party provides written authority from the data subject that they are acting on their behalf.
This could be ensuring that the appropriate section of our form has been signed or, that a letter has been provided or proof of a more general power of attorney.

b) Requests for information about children

Parents and guardians do not have an automatic right to access their children's files. Whilst the DPA 2018 sets the age of consent for children at 13, this is in relation to information society services and does not necessarily mean that the council has to seek the views of the child before releasing information to their parents or guardians. If a child is old enough to give informed consent, we would be guided by their wishes. The council will only disclose information to parents/guardians where this is in the best interests of the child.

3.12 Information Governance Officers

All Directorates have nominated Information Governance Officers (IGOs) who serve to represent all aspects of access to information within their functional area, including Freedom of Information (FOIA), Environmental Information Regulations (EIR) and Data Protection (DPA). Meetings are held at least quarterly. Further information about this role can be found in the Access to Information Policy.

4. Responding to requests

4.1 Clarifying the request

Where the council is unclear what a data subject is requesting, we will seek to obtain clarification. For example, where a DSAR is very broad, it may be challenging to locate the information the DPA does not allow public authorities to omit information from disclosure that is difficult to access or extend the time to respond. The council may ask the requester to clarify their request or to provide additional information to help the council locate the information they are looking for. The council cannot 'require' the requester to narrow the scope of the request, but we can ask them to provide context for their request, for example dates when processing is likely to have occurred or names of staff that have been involved. The council should request clarification as soon as possible; once the council seeks clarification we are not obliged to deal with the request until the clarification has been received.

4.2 Timescale for responding

The council must respond in one month to all individuals' rights requests. The clock starts on the day that the request is received by the council. The council is entitled to place a request on hold in the following situations:

- Clarification is requested;
- Identification is requested.

Should the request be placed on hold for one of the above reasons, the council is not obliged to deal with the request until the additional information has been provided. Once the council receives the additional information, the request is taken off hold and the clock is reset. This means that the council has one month from the date that clarification or, identification is provided.

The council is able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we must inform the individual within one month of the receipt of the request and explain why the extension is necessary. The circumstances in which this can be used will be updated as guidance from the Information Commissioner's Office (ICO) is made available

4.3 Charging for responses

The council must provide all information free of charge, however, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The council can charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent requests. This policy will be updated as further information and guidance is released from the ICO, however, in accordance with the Data Protection Act 2018, the council will apply the same principles of section 12, reasonable cost and effort, of the Freedom of Information Act 2000 when considering if it would be appropriate to levy a charge. Any fee issued by the council would be based on the administrative cost of providing the information only.

4.4 Locating and retrieving information

In accordance with our Article 30 obligations in the UKGDPR, the council has a Record of Processing Activities (RoPA), this register will help identify where information is held.

It is essential that all places where information could be held are searched, this includes:

- Electronic systems in use in your department/directorate;
- Shared Drives;
- Personal network drives (H Drives);
- Email accounts (this includes searching sent and deleted items);
- Backups and archives where these are held;
- Archived paper records.

4.5 Preparing the response

Third party information

The DPA states that you do not have to comply with a DSAR if to do so would mean disclosing information about another individual that can be identified, except where:

- The other individual has consented to disclosure; or
- It is reasonable to comply with the request without that Individual's consent.

It is essential that the council makes appropriate decisions in relation to disclosing third party information. You should always consult your IGO who will be able to provide you with further advice on what to do in these situations. Further information on exemptions can be found in section 5.

Redacting information

Once all information relating to the request has been located, this should be reviewed and redacted as appropriate. All redactions should be carried out in accordance with corporate guidance and checked by your manager before the information is disclosed.

Sending the information

Once the information has been gathered and the information for disclosure has been approved by a manager your IGO should send the response, or advise the requester their response is ready for collection. Where requests require information from more than one Directorate, the response will be coordinated by the Information Governance Team. The council's response must clearly explain the reasons why information has been withheld or redacted.

As a matter of good practice, the council should consult with the requester to identify how they would like to receive the information and, wherever possible we should try to comply with their request:

- By post, the council should use Royal Mail Special Delivery Service when sending DSAR responses;
- By email, the council should use secure email;
- Collection, the council should ask the requester to sign to confirm that they have received their response.

Copies of responses must be saved in the case management system so that we have a record of what was disclosed in case we receive a complaint regarding the handling of the request or the response received.

5. Exemptions

Exemptions are only applicable to DSARs. Subject access rights are very wide-ranging and there are no 'broad exemptions' when considering data for release. However, there are occasions where a data subject is not entitled to view the information held about them. The council must carefully consider the data to ensure that any exempt information is withheld or redacted.

Considerations for exemption include:

- Confidential references
- Prevention and detection of crime
- Third party information

- Legal professional privilege
- Management forecasting
- Negotiations

If you believe that you have information that should not be disclosed, you should first discuss this with your IGO who will be able to advise if information should be redacted. Your IGO can escalate the matter to the Exemptions Panel if they believe that it should be withheld.

6. Complaints

Details of how complaints regarding individuals' rights requests will be handled can be found in the council's Access to Information Policy.

7. Monitoring compliance and escalation

7.1 Overview

The council will monitor compliance in dealing with Individuals' Rights requests by ensuring that requests are closely monitored. The Access to Information Manager will review compliance in all areas and discuss issues with the relevant IGO and their manager where compliance is low. Persistent non- compliance will be escalated to the Information Access to Information Manager who will in turn escalate the matter to the Information Asset Owner in the first instance and the Corporate Management Board where agreed actions are not completed.

7.2 CMB will receive compliance reports

The Corporate Management Board (CMB) will receive quarterly reports on Individuals' Rights compliance. This will be submitted by the Access to Information Manager. The Corporate Management Board will receive monthly reports via email, this will also include details of open and overdue requests.

7.3 The IG Board will receive compliance reports

The Information Governance Board (IG Board) will receive quarterly reports on Individuals' Rights compliance, this will also include details of open and overdue requests. The Access to Information Manager will escalate incidents of persistent non-compliance as required.

7.4 IAOs will receive compliance reports

Information Asset Owners (IAO) will receive monthly reports on Individuals' Rights compliance via email. The Information Compliance Manager will escalate incidents of persistent non-compliance and provide detail of open and overdue requests where applicable.

8. Governance, approval and review

8.1 Information Governance Board

This policy and the commitment to a robust governance framework is subject to continuous, systematic review and improvement. This council-wide policy will be governed by the Information Governance (IG) Board, chaired by the Corporate Director of Resources, who is also the council's Senior Information Risk Owner. The IG Board reports directly into the Corporate Management Board.

8.2 Formal approval, adoption and review

This policy will be formally signed off by the Corporate Management Board. It will be reviewed on an annual basis by the Data Protection Officer who will feed back any issues to the IG Board.

The signatories agree with the content of this document.

Name	Role
David Hodgkinson	Director of Corporate Resources and SIRO
Peter Fehler	Acting Director of Law and Monitoring Officer
Leila Ridley	Head of Information Governance and DPO
Brad Pearton	Access to Information Manager