

# Information Sharing Agreement

## *Between LBB Electoral Registration Officer and LBB Revenues and Benefits*

### Contents

1.0 Process / Project.....	1
1.1 Responsibilities of parties involved.....	2
1.2 Assessment and Review .....	2
1.3 Termination of Agreement .....	2
2.0 Purpose & Benefits .....	2
2.1 Lawful basis for sharing data .....	3
2.2 Other relevant legislation .....	4
2.3 Consultation.....	4
3.0 Individuals .....	4
3.1 Data Subject Rights .....	4
3.2 Data Subject Requests .....	5
3.3 Complaints process .....	5
4.0 Data .....	6
4.1 Data handling and security .....	6
4.2 Secure sharing of personal data.....	6
4.3 Sharing under this agreement .....	7
4.4 Data Quality .....	7
4.5 Retention .....	7
4.6 Contractors .....	7
4.7 Data breach incidents .....	7
5.0 Risks .....	7
6.0 Signatures and Contacts.....	11
7.0 Appendix A: Information being shared .....	13
8.0 Appendix B: Data Protection & Caldicott Principles .....	15
Document Control.....	16
Version Control.....	16

### 1.0 Process / Project

This document agrees the sharing of information between LBB Electoral Registration Officer (ERO) and LBB Revenues and Benefits.

The parties will be processing personal data

- By being provided with data sets of C/Tax Empty/unoccupied/single persons discount data, it will allow the ERO to mark properties that are empty on the Register of Electors and also properties that have a single person registered against it. Receiving new resident data will enable the ERO to contact the new person and encourage them to register. Contact details, such as phone numbers and email addresses will be provided where held.

### 1.1 Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act.

Party	ICO number
LBB Electoral Services	Z832541X
LBB Revenues and Benefits	Z6665870

All parties have confirmed they have data protection and data security policies and procedures in place to ensure compliance with UK data protection laws.

It is the responsibility of each party to ensure that every employee processing personal data involved in this agreement knows how to obtain, use and share personal data in line with data protection law and the Data Protection Principles outlined in [Appendix B](#).

Parties to this agreement will ensure mandatory training is undertaken regularly by their officers to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.

Each organisation is responsible for their actions undertaken through this agreement.

### 1.2 Assessment and Review

A review of this information sharing agreement will take place if there is a significant change in the processing, unless otherwise agreed by the organisations' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not slipped, the benefits to the data subjects and organisations are being realised, and the procedures followed for information security are effective.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise.

### 1.3 Termination of Agreement

In the event of termination of this agreement each party may continue to hold information originating from other parties for which they are data controller.

## 2.0 Purpose & Benefits

This agreement covers the sharing of data for the purposes of C/Tax Empty/unoccupied/single persons discount and new resident data information held by Revenues and Benefits with Electoral services.

This information sharing is required for the purpose of performing its statutory electoral services duties.

### 2.1 Benefits of the processing

The work is intended to provide benefits in order to ensure electoral register records are accurate and up-to-date across the Borough, and to improve the standard of the services delivered.

The ERO also has a duty to send an Invitation to Register to new residents who have moved into an address. By being provided with weekly/monthly data sets of new residents this will allow the ERO to carry out their function in accordance by law.

Receiving contact details will assist in contacting potential electors via data means and therefore reducing the cost of printing and posting individual registration forms

### 2.2 Lawful basis for sharing data

Article 6 of the UKGDPR of the DPA2018 sets out the acceptable conditions for the processing and sharing of personal data.

The lawful basis conditions that apply to the purposes of this agreement are:

Article 6 (1)
(c) processing is necessary for compliance with a <b>legal obligation</b> to which the controller is subject
(e) processing is necessary for the performance of a task carried out in the <b>public interest</b> or in the exercise of official authority vested in the controller

The legislation that requires or allows the processing under this agreement is listed in the table below.

Legislation	Main purpose of Legislation
The Representation of People (England and Wales) Regulations 2001 – Section 35 states the following: Registration officer's right to inspect certain records 35.	(1) A registration officer is authorised to inspect, for the purpose of his registration duties, records kept (in whatever form) by— (a) an authority listed in paragraph (2) below, or (b) any person providing services to, or authorised to exercise any function of, any such authority. (2) Those authorities are— (a) the council by which he was appointed; and (b) any registrar of births and deaths. (3) A registration officer is



Legislation	Main purpose of Legislation
	authorised to make copies of information contained in such records. This means that the electoral registration officer can inspect and make copies of records kept in whatever form by its appointing council for the purposes of meeting registration duties; including any company or organisation, providing services to, or authorised to exercise any function of, the council
Local Government Finance Act 1992	administer and enforce Council Tax

### 2.3 Other relevant legislation

The actual disclosure of any personal data to achieve these objectives must also be conducted within the framework of the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence. Caldicott Principles also apply to all information sharing and they are listed in [Appendix B](#).

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who holds the information (data controller).

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

### 2.4 Consultation

None.

### 3.0 Individuals

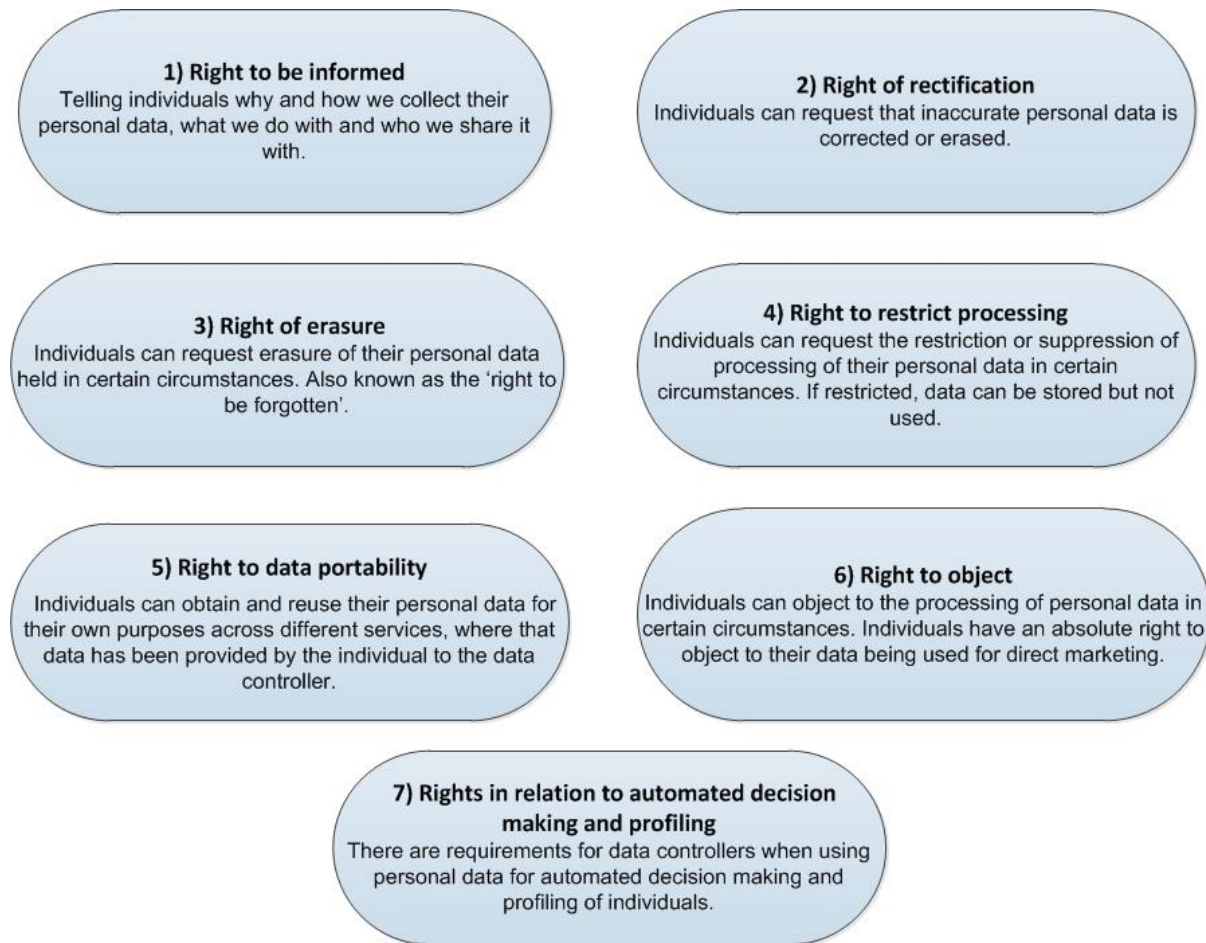
Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Each party agrees that they have undertaken a DPIA (Data Protection Impact Assessment), where they feel the processing meets the legislative criteria for a DPIA.

The table at [Appendix A](#) describes the data subjects and their relationship to the parties.

### 3.1 Data Subject Rights

Individuals have rights under data protection legislation. These rights, also known as Subject Access Rights, are:



All parties confirm that they obey the transparency requirements of UK\_GDPR and will issue appropriate privacy notices which inform the data subject what information is being processed, who it will be shared with under this agreement, the purposes for which it will be shared, and how long the data will be retained.

All parties confirm that they will make information available to data subjects regarding their data subject rights under the UK\_GDPR and the DPA2018.

### 3.2 Data Subject Requests

Each organisation must have in place appropriate policies and processes in place to handle data subject requests made in line with data protection law, to ensure they are responded to within deadline and in an appropriate manner.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), or withdraws their consent for processing (where consent is the lawful basis condition), the party that has been informed by the data subject will communicate this to the other parties. In each case each party is responsible for securely disposing of such information or limiting its processing.

### 3.3 Complaints process

Each party must have clear, fair and objective complaint procedures. Any concerns raised in relation to this agreement, must be passed to the Records and Information Management Services email [data.protection@barnet.gov.uk](mailto:data.protection@barnet.gov.uk)

#### 4.0 Data

The information to be shared under this agreement is C/Tax Empty/unoccupied/single persons discount and new/change of resident data, including contact details. It is described in more detail in Appendix A.

It does not include special category personal data or criminal data.

All parties confirm they have considered the possibility of using anonymised data and it was not viable. During the sharing process all parties will consider whether data can be pseudonymised.

The sharing will happen weekly/monthly/ad hoc when required.

Data will be sent as a CSV file. Address to be separated into columns – Address 1, Address 2, Address 3 and postcode. Names will be in separate columns – First name, surname. Each named entry for a property will be on a separate line. Codes for benefits, changes etc will be in separate columns.

Contact details will be provided such as telephone number and email address.

The data will/will not be transferred outside the UK by any of the parties.

#### 4.1 Data handling and security

All parties must have in place appropriate technical and organisational security measures to ensure the confidentiality, integrity and availability of personal data and protect against accidental loss, destruction, damage, alteration or disclosure. These measures must be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the personal data and having regard to the nature of the personal data which is being processed.

The London Borough of Barnet works towards ISO 27001, the International Standard for Information Security Management. There is an expectation that all parties will either be working toward or meeting a similar standard of security.

#### 4.2 Secure sharing of personal data

Personal data must be shared securely. All parties agree that:

- any transfers of personal data will be appropriately packaged and securely transferred, to mitigate any loss or unlawful disclosure of data.
- all staff having access to the data will be security checked where appropriate, in line with best practice.
- any individual no longer required to have access will promptly have such access revoked by the relevant employer.

- ID passes are required and worn in the facilities of each party, to ensure access to the premises is legitimate. Any person without ID can and will be challenged.
- all data held electronically will be stored in a secure network area and appropriate back-up functionality. The area/system will be auditable so that it is possible to establish who has accessed the system.
- all laptops, computers, and any other portable devices will be encrypted.
- paper records will be kept to a minimum and kept secure, whether in the office, home or during transit. Appropriate security methods will be applied when storing or disposing of paper records.

### 4.3 Sharing under this agreement

The data described in this agreement will be shared on an LBB drive that both parties can access or on a Teams channel for larger ad hoc files. Access to these files will be restricted to senior staff who are DBS checked where appropriate in line with best practice. The table in [Appendix A](#) provides more detail about the sharing processes.

Email is not generally a secure method of transferring personal data. Personal data should not be transferred via email except through approved, secure methods.

### 4.4 Data Quality

Data quality will be assured through follow up checks throughout the annual canvass period.

### 4.5 Retention

Electoral Services retention period of 3 months

Revenues and Benefits retention period of 10 years

### 4.6 Contractors

All parties agree that they will undertake appropriate data protection due diligence checks with any contractors/data processors they employ, that a written agreement will be in place with each data processor, and that all data processors will be bound by this agreement.

### 4.7 Data breach incidents

All parties must have a clear policy and procedure for reporting and handling data protection breaches or data loss incidents. All parties agree to inform the other parties as appropriate if the incident has an impact on the processing of the other parties.

## 5.0 Risks

An assessment of the risks involved in sharing and handling information under this agreement has been undertaken and actions to mitigate risks to the confidentiality, integrity and

accessibility of the data are listed below. These risks have been incorporated in risk registers in line with each party's risk processes.

The table below provides a high-level assessment of the most significant risks associated with the sharing of information under this agreement, and any mitigations agreed by the parties.

This agreement does not involve high-risk processing of C/Tax Empty/unoccupied/single persons discount and new resident data. There are no known issues and/or public concerns with this type of processing and sharing and is standard practice across Local Authorities.



**Risk Table**

If any high risks are identified, the DPO must review them and the proposed options to mitigate.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk	Mitigation options to reduce or eliminate risk	Effect on risk	Residual risk	Measure reviewed by DPO?
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high		Eliminated reduced accepted	Low medium high	Yes/No
System malfunction/hacking	1	3	3	Data stored on a secured Barnet IT controlled network server and password protected. It can only be accessed by staff with authorised access to the Electoral software system.	1	1	No
Additional Personal Data is sent to LBB ERO in error	1	3	3	Sense check of data provided to ensure monthly from LBB Revenues and Benefits extract only contains relevant data built into project plan.	1	1	No
Sending personal data to incorrect recipient	1	3	3	Parties to work together in the event of a complaint related to the accuracy of data used in the Project.	1	1	No

Information Sharing Agreement

---

Computing devices containing personal data being lost or stolen	1	3	3	Data not held on computing devices only LBB server in a folder with access on a needs to know basis and extract which is password protected	1	1	No
Personal Data not deleted at the end of use by Electoral Services	1	3	3	Deletion built into project plan.	1	1	No

### 6.0 Signatures and Contacts

This agreement describes procedures that provide a secure framework for the sharing of data between signature parties. By signing this agreement parties accept that it is their responsibility to ensure their actions are lawful and comply with obligations described in this agreement.

Name	Role/Responsibility	Organisation	Signature	Date
██████████	Head Of Finance - Exchequer  Strategy and Resources -	LBB	██████████	██████████
██████████	Electoral Services Manager	LBB (On behalf of ERO)	██████████	██████████

Officers holding data protection and data security roles must be consulted when drafting this agreement. Their details should be entered below.

Name	Role/Responsibility	Organisation	Contact Details (email & phone)	Comments on the agreement/ processing	Date
	eg DPO, Caldicott Guardian, FOI/SAR lead				
John E Bailey	ERO	LBB	Electoral Registration Office <a href="#">Electoral.Registrati</a>		

Information Sharing Agreement

---

			<a href="mailto:onOffice@Barnet.gov.uk">onOffice@Barnet.gov.uk</a>		
Lucy Martin	DPO	LBB	<a href="mailto:Data.protection@barnet.gov.uk">Data.protection@barnet.gov.uk</a>		



**7.0 Appendix A: Information being shared**

**Types of data subjects** Tick all that apply.

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Customers or Service users | <input type="checkbox"/> Traders or people subject to inspection | <input type="checkbox"/> Recipient of benefits                                    |
| <input type="checkbox"/> Service providers / Contractors       | <input type="checkbox"/> People captured on CCTV                 | <input type="checkbox"/> Councillors, MPs, elected officials                      |
| <input checked="" type="checkbox"/> Residents                  | <input type="checkbox"/> Representative of another organisation  | <input type="checkbox"/> Volunteers   |
| <input type="checkbox"/> Complainants                          | <input type="checkbox"/> Licence and permit holders              | <input type="checkbox"/> Professional adviser or consultant (eg doctor or lawyer) |
| <input type="checkbox"/> Claimants                             | <input type="checkbox"/> Employees (previous or current)         | <input type="checkbox"/> Any  |

Are the data subjects considered vulnerable? eg children or abuse victims?	Volume of data subjects	What control do data subjects have over the processing/sharing of their data? NB: for much of our processing the answer will be none	What is the relationship between the organisation(s) and the data subjects? eg is the organisation in a position of power? Do data subjects have any choice about working with us?
No	The whole borough	Able to access Data Subject Rights	No, it's a statutory requirement for Electoral Services to carry out the Annual canvas

Information Sharing Agreement

What information is being shared	Who in the organisation shares the information? eg Social worker	How is the information shared? eg secure email	Who in the organisation receives the information? eg DWP Disability Employment Advisers	What happens with the information when it is received? eg stored in DWP database	How long will the data be kept? eg retained for 5 years
C/Tax Empty/unoccupied/single persons discount and new/change of resident data, including contact details for residents from LBB - Council to LBB - Electoral Services.	LBB - Council Tax	Shared on an LBB drive that both parties can access or on a Teams channel for larger ad hoc files. Access will only be given to senior members of staff with access to that shared drive or Teams channel.	LBB - Electoral Services (ERO)	The data will be imported into Electoral Services Electoral Management System (EMS) for data matching purposes, to ensure the electoral register is up to date and accurate and to encourage new elector registrations.	The data will be stored on shared drive. The data will be retained for a period of three months

## 8.0 Appendix B: Data Protection & Caldicott Principles

### The Principles as described in Article 5 of the General Data Protection Regulation.

**1) Fair & Lawful**  
processed lawfully, fairly and in a transparent manner in relation to the data subject

**2) Purpose limitation**  
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

**3) Data minimisation**  
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

**4) Accuracy**  
accurate and, where necessary, kept up to date; Inaccurate data must be erased or rectified without delay

**5) Storage limitation**  
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

**6) Integrity & Confidentiality**  
secured through appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

### The Caldicott Principles

**Principle 1**  
**Justify the purpose(s) for using confidential information**  
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2**  
**Don't use personal confidential data unless it is absolutely necessary**  
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3**  
**Use the minimum necessary personal confidential data**  
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4**  
**Access to personal confidential data should be on a strict need-to-know basis**  
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

**Principle 5**  
**Everyone with access to personal confidential data should be aware of their responsibilities**  
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6**  
**Comply with the law**  
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7**  
**The duty to share information can be as important as the duty to protect patient confidentiality**  
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

Further information can be found in the [Caldicott Guardian Pages](#) on the government website.

**Document Control**

<b>Document Description</b>	Information Sharing Agreement between the London Borough of Barnet (on behalf of the ERO) and Revenues and Benefits (to be read in conjunction with and in accordance with the LBB Information Sharing Protocol)		
<b>Version</b>	3.0		
<b>Date Created</b>	29.09.23		
<b>Status</b>	FINAL		
<b>Authorisation</b>	Name	Signature	Date
<b>Prepared By:</b>	Richard Carter	R Carter	29.09.23
<b>Checked By</b>	██████	██████	3.10.23

**Version Control**

Version number	Date	Author	Reason for New Version
1.0			Information Sharing Agreement
2.0	05.10.18	R Carter	GDPR Compliant ISA Template
3.0	27.10.23	R Carter	Updated Data Sharing Agreement template