Data Protection Policy
&
Procedures

(For employees/workers, elected members and data processors)

Document Ref.	Data Protection Policy
Version:	1.0
Dated:	August 8, 2018
Document Author:	Gonzalo del Castillo
Document Owner:	IG

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	August 8, 2018	G. del Castillo	New policy

Distribution

Name	Position	Date circulated
Matt Ginn and IG Group	Head of Information Governance and DPO	03/07/2018
IDIG	Intelligence Digital and Information Governance	13/07/2018

Approval

Name	Position	Date of sign off
Jackie Belton	Senior Information Risk Owner (SIRO) Strategic Director, Corporate Resources	August 8, 2018

Contents

1 INTRODUCTION 4
1.1 DEFINITIONS 4
1.2 KEY ROLES AND RESPONSIBILITIES 5

2 THE DATA PROTECTION PRINCIPLES 7
2.1 LAWFULNESS FAIRNESS AND TRANSPARENCY 7
2.2 PURPOSE LIMITATION 8
2.3 DATA MINIMIZATION 9
2.4 ACCURACY 9
2.5 STORAGE LIMITATION 10
2.6 INTEGRITY AND CONFIDENTIALITY 11
2.6.1 DATA SECURITY – TRANSFERRING PERSONAL DATA AND COMMUNICATIONS 11
2.6.2 DATA SECURITY – STORAGE 11
2.6.3 DATA SECURITY – DISPOSAL 12
2.6.4 DATA SECURITY – USE OF PERSONAL DATA 12
2.6.5 DATA SECURITY – IT SECURITY 12
2.6.6 DATA SECURITY – PERSONAL DATA BREACHES 13

2.7 ACCOUNTABILITY 13
2.7.1 Recordkeeping 14
2.7.2 Data Protection Impact Assessments (DPIA) 14

3. LAWFUL BASIS 14
3.1 CONSENT 15
3.2 CONTRACT PERFORMANCE 16
3.3 COMPLIANCE WITH A LEGAL OBLIGATION 17
3.4 PROTECTION OF VITAL INTERESTS 17
3.5 PUBLIC TASK 17
3.6 LEGITIMATE INTERESTS 18

4. SPECIAL CATEGORIES 19

5. RIGHTS OF DATA SUBJECTS 20
5.1 THE RIGHT TO BE INFORMED 20
5.2 THE RIGHT OF ACCESS 21
5.3 THE RIGHT TO RECTIFICATION 21
5.4 THE RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN') 21
5.5 THE RIGHT TO RESTRICT PROCESSING 22
5.6 THE RIGHT TO DATA PORTABILITY 22
5.7 THE RIGHT TO OBJECT 22
5.8 AUTOMATED DECISION-MAKING AND PROFILING RIGHTS 23

6. ORGANIZATIONAL MEASURES 23

7. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA 24

Appendix A – Privacy Notice Procedure 25
Appendix B – Report a Data Breach to Lambeth Council 29
Appendix C – Consent Article 30
Appendix D – Legitimate Interests Assessment Procedure - ICO Sample LIA Template 33

1. INTRODUCTION

This Policy sets out the obligations of Lambeth Council (the "**data controller**"), regarding the collection, processing, transfer, storage, and disposal of personal data, as well as the rights of data subjects under EU Regulation 2016/679 General Data Protection Regulation (hereinafter the 'GDPR') and the Data Protection Act (2018) (hereinafter the 'DPA').

The general principles, checklists and procedures referred to and set out herein apply to and must be followed at all times by Lambeth Council, its employees, agents, contractors, or other parties working for or providing services to Lambeth Council. Given the number and variety of services and processes handled by or on behalf of the Council, there is no one-size-fits-all procedure suitable for all processes. Therefore, all Heads of Service are responsible for the dissemination of this policy to their staff and where appropriate, the creation and implementation of procedures and training specific to their service in accordance with the principles of this policy (see checklists within this policy for guidance).

All organisations working with personal data face a number of risks and have a duty to identify such situations and take the appropriate measures to remedy them. Lambeth Council is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The aim of this policy is to help create a culture of awareness and encourage you to actively participate and raise issues which concern all and any aspects when it comes to working with personal data. For any questions regarding compliance with data protection regulations please visit the Information Governance Team's page on Lamnet or contact Lambeth Council's Data Protection Officer (DPO) infogov@lambeth.gov.uk.

1.1 DEFINITIONS

'Controller' (Lambeth Council) means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

'**Process'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'**Processing**' refers to the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

'**Personal Data**' means any information relating to an identified or identifiable natural person (also known as the '**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 Breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'**Supervisory Authority**' means ICO (The Information Commissioner's Office) as far as Lambeth Council's processing activities are concerned.

1.2 KEY ROLES AND RESPONSIBILITIES

All staff at Lambeth Council have a prime responsibility to observe and understand the data protection principles in this policy.

Policies, training and relevant communications will be provided to ensure that staff are aware of their obligations regarding Data Protection as defined by the GDPR and Data Protection Act, Freedom of Information and information management. More detailed training will be provided for specific groups of staff whose duties mean that they handle large amounts of sensitive data on a daily basis. Each individual is responsible for ensuring that they receive this training and that they have read and understood the relevant policies.

Key Roles

There are a number of senior roles within Lambeth Council that have key data protection responsibilities.

Enterprise Architect

The Enterprise Architect is responsible for designing the Council's information architecture – including its logical and physical data assets and data management resources. The Enterprise Architect will work with key stakeholders both internal and external to ICT (directors, service managers, business liaison managers and subject matter experts) to build a holistic view of the Lambeth Council's strategy, processes, information, and information technology assets. The role of the Enterprise Architect is to take this knowledge and ensure that the business and ICT are aligned.

Directors and Heads of Service

Directors and Heads of Service are responsible for considering Information Governance implications when planning to out-source services, work with partners or commission new technologies or major structural changes. Records Management considerations must be specified at the outset with suppliers and partners and built into service and technology specifications.

Caldicott Guardian

The Caldicott Guardian position is held by the Director of Public Health, who is the senior person responsible for protecting the confidentiality of individuals using care and support services and enabling appropriate information sharing. Good record management practice is a key consideration for the Caldicott Guardian in discharging their responsibilities. The Caldicott Guardian is the person with overall responsibility for protecting the confidentiality of personal data across Lambeth Council. The Caldicott Guardian plays a key role in ensuring that Lambeth Council and partner organisations abide by the highest level for good record keeping standards for handling personal data.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) role is currently held by the Strategic Director, Corporate Resources. The role:

- Is accountable for information risk management
- Fosters a culture for protecting and using data
- Provides a focal point for managing information risk and incidents
- Is concerned with the management of all information assets

The SIRO has overall accountability for the risk management requirements outlined in this policy and will oversee Records Management with specific interest in the reliability and protection of data in line with the Data Protection Act.

Information Asset Owners (IAO)

IAOs are senior / responsible individuals working in a relevant business area. Their role is to understand what information is held within their business area, what is added and what is removed, how information is moved, who has access and why. They will ensure adequate records are in place which document their areas activities. IAOs shall establish, maintain and update the Information Asset Register (IAR) and retention periods for the personal data processed by their service area(s) (see section 2.5 Storage Limitation). The quality of record management to support the maintenance of information assets is a key responsibility of an IAO.

The IAO will be responsible for ensuring that record management is incorporated into all relevant operational procedures and that these procedures are properly implemented and monitored regularly.

Information Asset Administrators (IAA)

The Information Asset Administrators (IAAs) will have day to day responsibility for record management practice in relation to their information assets and will need to ensure that all data protection principles and this policy are fully observed and applied operationally and understood by staff in their operational area. Specifically and within their own service areas, IAAs will be responsible for handling, coordinating and responding to Data Subject Requests (see Data Subject Request Policy & Procedure). Any issues that may affect record management must be escalated to Information Asset Owners to assess and plan any mitigating actions.

Data Protection Officer (DPO)

The DPO is the Head of Information Governance and is responsible for ensuring the organisation meets its statutory and corporate responsibilities and engenders trust from the public in the management of their personal information. The DPO is accountable for overseeing monitoring and spot check processes in relation to all policies and reporting to the Senior Information Risk Owner on compliance with the Council's policies.

Information Security Officer

The Information Security Officer is responsible for providing information security advice to the Council. Information security has a key role in supporting good record management practice, ensuring that records cannot be corrupted or changed without agreed access and permissions. Any security issues impacting on the integrity of records will be reported to the relevant IAO for resolution.

Intelligence, Digital and Information Governance (IDIG)

The Intelligence Digital Information Governance management sub-group will oversee the management of the Information Governance Framework with senior representation from across Lambeth Council to monitor compliance and continuous improvement around information governance. Although the membership of the board will vary over time, it shall always include a representative from each of the directorates.

The current IDIG group includes the following representatives:

- Strategic Director, Corporate Resources (Chair)
- Director of Legal Services and HR
- Director of Environment
- Director of Public Health
- Director of IT and Customer Services
- Director of Communications & Improvement, Strategy & Commissioning – Children
- Head of Service, Business Transformation
- Interim Director of Policy and Communications
- Consultant in Public Health
- Strategic Lead – Crime & Disorder
- Head of Information Governance
- Head of Policy and Partnerships

2. THE DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the GDPR and the DPA, which set out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

2.1 Lawfulness Fairness and Transparency

The GDPR and the DPA seek to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject.

For processing of personal data to be lawful, you need to identify specific grounds for the processing. This is called a ‘lawful basis’ for processing, and there are six options which depend on your purpose and your relationship with the individual (see section 3).

In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should and if so, how much personal data is necessary for the particular processing purpose.

Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair (see section 5.1).

The principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand, and that clear and plain language be used. The requirement that information “must be concise and transparent” means that it should be presented efficiently and succinctly. To this end, the use of ‘layered’ privacy notices is allowed and encouraged, enabling the data subject to navigate to a particular section of the privacy notice. (see Appendix A for Privacy Notice Procedure).

CHECKLIST:

Lawfulness

☐ We have identified an appropriate lawful basis for our processing (see section 3).

☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data (see section 4).

Fairness

☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact (see sections 2.7.2 and 3.6).

☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified (see sections 2.2 and 3.6).

☐ We do not deceive or mislead people when we collect their personal data (see sections 5.1 and 5.2).

Transparency

☐ We are open and honest, and comply with the transparency obligations of the right to be informed (see section 5.1 and Appendix A on privacy notices).

2.2 Purpose Limitation

Data subjects shall be kept informed at all times of the purpose or purposes for which Lambeth Council uses their personal data.

Be clear about what your (service area) purposes for processing are from the start.

Record your purposes as part of your documentation obligations and specify them in your privacy notice(s) to individuals (see section 5.1).

Only use the personal data for a new purpose if either this is compatible with the original purpose, consent is given by the data subject (see section 3.1), or there is a clear basis in law.

What is a 'compatible' purpose?

The GDPR specifically says that the following purposes should be considered to be compatible purposes:

•archiving purposes in the public interest;

•scientific or historical research purposes; and

•statistical purposes.

Checklist:

☐ We have clearly identified our purpose or purposes for processing (see section 5.1).

☐ We have documented those purposes.

☐ We include details of our purposes in our privacy notice(s) to individuals.

☐ We regularly review our processing and, where necessary, update our documentation and

our privacy notice(s) to individuals.

☐ If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose or we get specific consent for the new purpose (see section 3.1).

2.2 Data Minimization

Lambeth Council will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed.

Identify the minimum amount of personal data needed to fulfil the processing purpose and establish appropriate (service area specific) procedures to ensure that you **only collect and hold the personal data you need**. (Tips: Do you absolutely need 'special category' information such as ethnicity or religion for the specific processing purpose? If so, it must meet one of the conditions in section 4. Alternatively, consider anonymising or processing such data in an anonymous way at the time of collection).

Checklist:

☐ We only collect personal data we actually need for our specified purposes.

☐ We have sufficient personal data to properly fulfil those purposes.

☐ We periodically review the data we hold, and delete anything we don't need.

2.4 Accuracy

Lambeth Council shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject (see section 5.3).

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay at the service-area level to amend or erase that data, as appropriate.

What about records of mistakes?

Lambeth Council may legitimately need records to accurately reflect the order of events (i.e. if a charge was imposed, but later cancelled or refunded). Keeping a record of the mistake and its correction might also be in the individual's best interests.

CHECKLIST:

☐ We ensure the accuracy of any personal data we create.

☐ We have appropriate measures in place to check the accuracy of the data we collect, and we record the source of that data.

☐ We have a system in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.

☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.

☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data (see section 5.3).

☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

2.5 Storage Limitation

The GDPR and the DPA do not set specific time limits for different types of data. This is up to Lambeth Council and/or the specific service area(s), and will depend on how long the data is needed for the specified purposes.

Lambeth Council shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

To comply with documentation requirements, each Information Asset Owner within (or service provider to) Lambeth Council needs to establish and document standard retention periods for different categories of information held wherever possible. Each IAO shall establish a system for ensuring that they keep to these retention periods in practice, and for reviewing retention at appropriate intervals. Each service area must also be flexible enough to allow for early deletion if appropriate. For example, if a record is not actually being used, the need to retain it should be reconsidered. Retention periods as established and periodically reviewed by IAOs must be communicated to the Information Governance Team to be included in the council-wide retention schedule (see Lambeth Council's Records Management and Retention Policy).

CHECKLIST:

☐ We know what personal data we hold and why we need it.

☐ We carefully consider and can justify how long we keep personal data.

☐ We keep a record of our own retention periods where possible (each service area shall determine, establish and document the retention periods applicable to their processes in accordance to their specific processing needs or as required by law).

☐ We regularly review our information and erase or anonymise personal data when we no longer need it.

☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

2.6 Integrity and Confidentiality

Lambeth Council shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, disclosure or damage. Further details of the technical and organisational measures which shall be taken are provided below (also refer to Lambeth Council's Cyber Security Strategy and Information Security Policy).

2.6.1 Data Security - Transferring Personal Data and Communications

Lambeth Council shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

1. All emails containing personal data must be encrypted;
2. All emails containing personal data must be marked "confidential";
3. Personal data may be transmitted over secure networks or encrypted transmissions only;
4. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
5. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
6. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient; and
7. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

2.6.2 Data Security – Storage

Lambeth Council shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
3. All personal data stored electronically should be backed up. All backups should be encrypted; and
4. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Lambeth Council where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to Lambeth Council that all suitable technical and organisational measures have been taken).

2.6.3 Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

2.6.4 Data Security - Use of Personal Data

Lambeth Council shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Lambeth Council requires access to any personal data that they do not already have access to, such access should be formally requested;

2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of Lambeth Council or not, without proper authorisation or legitimate access rights; Access to personal data is granted on a principle of least required access using role based access controls ('RBAC'; See Lambeth Council Cyber Security Strategy).

3. Personal data must be handled with care at all times and should not be left unattended (i.e. paper files) or on view to unauthorised employees, agents, sub-contractors, or other parties at any time; All personal data in hardcopy form must remain in the work area; If removed (i.e. taken home by worker with proper access or 'RBAC') a record must be kept of the details of the specific records removed.

4. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

5. Where personal data held by Lambeth Council is used for marketing purposes, it shall be the responsibility of the service area promoting the marketing to ensure that they either complete and record a Legitimate Interest Assessment or obtain appropriate consent (and that no data subjects have opted out, whether directly or via a third-party service).

2.6.5 Data Security - IT Security (See Lambeth Council Cyber Security Strategy)

Lambeth Council shall ensure that the following measures are taken with respect to IT and information security:

1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by Lambeth Council is designed to require such passwords;
2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Lambeth Council, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
3. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Lambeth Council's IT staff shall be responsible for installing any and all security-related updates; and

4. No software may be installed on any Company-owned computer or device without prior IT approval.

2.6.6 Data Security – Personal Data Breaches

If you become aware of a personal data breach, report it immediately by calling Lambeth Council's 24/7 dedicated line 0207 926 9111 and providing the following information (see Reporting Form in Appendix B):

1. The date and time that the breach was discovered;
2. The date and time that the breach is believed to have occurred
3. The data items included (i.e. names, addresses, bank details, biometrics)
4. The volume of data involved
5. The categories and number of data subjects affected
6. The nature of the breach (i.e. theft, accidental destruction, disclosure)
7. Whether the personal data was encrypted
8. If encrypted, the strength of the encryption used
9. To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
10. The actions that have been taken to manage the impact of the breach
11. Contact details of the person handling the breach within our organisation
12. Any other factors that are deemed to be relevant

The following two paragraphs are intended for the DPO:

i. If a personal data breach occurs and that breach is likely to result in **a risk** to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the **Data Protection Officer must ensure** that the **Information Commissioner's Office is informed** of the breach without delay, and in any event, **within 72 hours** after having become aware of it pursuant to Lambeth Council's Personal Data Breach Notification Policy and Procedure.

ii. In the event that a personal data breach is likely to result in **a high risk** (that is, a higher risk than that described in the above paragraph) to the rights and freedoms of data subjects, the **Data Protection Officer must ensure** that all affected **data subjects are informed** of the breach directly and **without undue delay** pursuant to Lambeth Council's Personal Data Breach Notification Policy and Procedure.

2.7 ACCOUNTABILITY

Lambeth Council's Data Protection Officer (DPO) is the Head of Information Governance, (infogov@lambeth.gov.uk or 0207 926 7717).

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Lambeth Council's other data protection-related policies, and with the GDPR and the DPA.

2.7.1 Recordkeeping

Each service area in Lambeth Council shall keep written internal records of all personal data they collect, hold, use, share and process, which shall incorporate the following information:

1. The specific service area and process owner (Information Asset Owner or Information Asset Administrator), as well as any applicable third-party data processors;
2. The purposes for which it collects, holds, uses, shares and processes personal data;
3. The legal basis or bases for each processing purpose.
4. Details of the categories of personal data collected, held, used, shared and processed by the services area, and the categories of data subject to which that personal data relates;
5. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
6. Details of how long personal data will be retained by the service area; and
7. Detailed descriptions of all technical and organisational measures taken by the service area to ensure the security of personal data.

2.7.2 Data Protection Impact Assessments (DPIAs)

Lambeth Council service areas shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and/or **whenever the processing involved is likely to result in a high risk to the rights and freedoms of data subjects** under the GDPR and DPA.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

1. The type(s) of personal data that will be collected, held, and processed;
2. The purpose(s) for which personal data is to be used;
3. The service area's/processing objectives;
4. How personal data is to be used;
5. The parties (internal and/or external) who are to be consulted;
6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
7. Risks posed to data subjects;
8. Risks posed both within and to service areas/Lambeth Council; and
9. Proposed measures to minimise and handle identified risks.

For further guidance on how to carry out a DPIA and its format, see Lambeth Council's DPIA Procedure and Template document provided in the Information Governance Team's Page.

3. LAWFUL BASIS

The GDPR and the DPA require that processing of personal data shall be lawful if at least one of six lawful bases applies **before starting to process** (i.e. collecting) personal data.

It may be possible that more than one basis applies to the processing because you have more than one purpose and if so, you should make this clear to the data subject prior to

processing their personal data.

How to decide which lawful basis applies will depend on the specific purposes and the context of processing. No one basis is always better nor applicable across every process.

Factors to consider include: What are you trying to achieve?; Can you reasonably achieve it in a different way ? Do either you or the data subject have a choice over whether or not to process the data? (As a public authority, certain processing activities may fall under either 'public task' or 'legal obligation', in which case a certain law will require the processing).

CHECKLIST:

☐ We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.

☐ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.

☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.

☐ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

☐ Where we process special category data, we have also identified a condition for processing special category data, and have documented this (see section 4).

☐ Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

The six lawful bases are:

3.1 **Consent** (See Appendix C 'Consent GDPR Article by RDM')

The data subject has given **consent** to the processing of their personal data for one or more specific purposes.

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment.

When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR and the DPA, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.

However, even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and would not meet the 'fairness' obligation.

In order to be valid, **consent must be: freely given, specific, informed and unambiguous**.

The element "free" implies real choice and control for data subjects. As a general rule, if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.

Consent will not be free in cases where there is any element of compulsion, pressure/inability to exercise free will or conditionality to provide services (i.e. if the services are conditional on

the individual's consent, then it is not true consent and is therefore invalid – a different lawful basis for processing must applied).

CHECKLIST:

Asking for consent

☐ We have checked that consent is the most appropriate lawful basis for processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask people to positively opt in.

☐ We don't use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we're going to do with it.

☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

☐ We name our organisation and any third party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Managing consent

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.

☐ We have methods in place to refresh consent at appropriate intervals, including any parental consents.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don't penalise individuals who wish to withdraw consent.

3.2 **Contract performance**

The processing is **necessary for the performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them.

If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get a separate consent.

If processing of a special category data is necessary for the contract, you also need to identify a separate condition for processing this data (see section 4).

3.3 **Compliance with Legal Obligation**

The processing is necessary for **compliance with a legal obligation** to which the data controller is subject.

You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation, but you should be able to **identify the specific legal provision or an appropriate source of guidance** that sets out your obligation.

Legal obligation is the applicable basis if you are obliged to process personal data to comply with the law (i.e. processing personal financial information for HMRC reporting or fraud detection).

Processing on the basis of legal obligation does not entitle the individual to the right to erasure, data portability or the right to object.

3.4 **Protection of Vital Interests**

The processing is necessary to **protect the vital interests** of the data subject or of another natural person.

If you need to process the personal data to protect someone's life (i.e. certain children or adult services), you are likely to be able to rely on vital interests as your lawful basis. This lawful basis is very limited in its scope, and generally only applies to matters of **life** and **death**, such as emergency medical care (when you need to process personal data for medical purposes but the individual incapable of giving consent to the processing).

The vital interests legal basis may be relevant however, if it is necessary to process a parent's personal data to protect the vital interests of a child.

You cannot rely on vital interests for health data or other special category if the individual is capable of giving consent, even if they refuse their consent.

In most cases the protection of vital interests is likely to arise in the context of health data. Since this is one of the special categories of data it means you will also need to identify a condition for processing special category date (see section 4).

3.5 **Public Task**

The processing is necessary for the performance of a task carried out in the **public interest or in the exercise of official authority** vested in the data controller (i.e. local government tasks, functions, duties or powers). The focus should be on demonstrating either that you are carrying out a task in the public interest, or that you are exercising official authority. The nature of the actual function however, not the nature of the organisation, should determine whether the task is in the public interest.

3.6 **Legitimate Interests**

The processing is necessary for the purposes of the **legitimate interests** pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as public authority.

It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact. If you are relying on legitimate interests, you are taking on extra responsibility for protecting people's rights and interests.

There are three elements to the legitimate interests basis '**balancing test**':

1. identify a legitimate interest;
2. show that a processing is necessary to achieve it; and
3. balance against the individual's interests, rights and freedoms.

You must keep a record of your **legitimate interests assessment procedure** (or 'LIA', see Appendix D for the ICO recommended template).

The interests can be commercial, individual or broader societal benefits as long as the processing is necessary.

CHECKLIST:

☐ We have checked that legitimate interests is the most appropriate basis.
☐ We understand our responsibility to protect the individual's interests.
☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
☐ We have identified the relevant legitimate interests.
☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
☐ If we process children's data, we take extra care to make sure we protect their interests.
☐ We have considered safeguards to reduce the impact where possible.
☐ We have considered whether we can offer an opt out.
☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
☐ We keep our LIA under review, and repeat it if circumstances change.
☐ We include information about our legitimate interests in our privacy information.

4. SPECIAL CATEGORIES

For 'Special Categories' of data, it is important to check both electronic and paper forms and collect this information only if necessary and if it complies with the below requirements. Otherwise, consider either not collecting the special category information or doing so in an anonymous way (i.e. use separate form not tied or linked to an individual's personal information).
Personal data falls under a "special category" when it concerns the subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation. **Both a lawful basis (see section 3 above) and at least one of the following conditions are needed prior to processing special category data**:

1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes;
2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;
3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
5. The processing relates to personal data which is clearly made public by the data subject;
6. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
7. The processing is necessary for substantial public interest reasons, on the basis of EU or UK law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
8. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or UK law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
9. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. THE RIGHTS OF THE DATA SUBJECTS

The GDPR and the DPA set out the following rights applicable to data subjects:

1. **The Right to be Informed**
2. **The Right of Access**
3. **The Right to Rectification**
4. **The Right to Erasure ('Right to be Forgotten')**
5. **The Right to Restrict Processing**
6. **The Right to Data Portability**
7. **The Right to Object**
8. **Automated Decision-Making and Profiling Rights**

5.1 The Right to be Informed

Lambeth Council service areas shall inform every data subject in a timely manner:

1. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
2. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose;
3. If the personal data is used to communicate with the data subject, when the first communication is made; or
4. If the personal data is to be transferred to another party, before that transfer is made; or
5. As soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided prior to any personal data processing activity (see **privacy notice procedure** and example of 'layered' notice in Appendix A)

1. Lambeth Council contact details including, but not limited to, the identity of its Data Protection Officer;
2. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
3. Where applicable, the legitimate interests upon which Lambeth Council is justifying its collection and processing of the personal data;
4. The categories of personal data collected and processed;
5. Where the personal data is to be transferred to one or more third parties, details of those parties/recipients;
6. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;
7. Details of data retention;
8. Details of the data subject's rights under the GDPR and the DPA;
9. Details of the data subject's right to withdraw their consent to Lambeth Council's processing of their personal data at any time;
10. Details of the data subject's right to complain to the Information Commissioner's

Office;

11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
12. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

5.2 The Right of Access (See Lambeth Council's Data Subject Request Policy and Procedure)

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Lambeth Council holds about them, what it is doing with that personal data, and why.

Data subjects may find a form on our website: (insert Lambeth online form), although the GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request either verbally or in writing.

Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to Lambeth Council's Data Protection Officer at infogov@lambeth.gov.uk.

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed within one month of the request.

Lambeth Council does not charge a fee for the handling of normal SARs. Lambeth Council reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

5.3 The Right to Rectification

Data subjects have the right to require Lambeth Council to rectify any of their personal data that is inaccurate or incomplete.

Lambeth Council shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Lambeth Council of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed within one month of the request.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

5.4 Right to Erasure

Data subjects have the right to request that Lambeth Council erases the personal data it holds about them in the following circumstances:

1. It is no longer necessary for Lambeth Council to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
2. The data subject wishes to withdraw their consent to Lambeth Council holding and processing their personal data;
3. The data subject objects to Lambeth Council holding and processing their personal data (and there is no overriding legitimate interest to allow Lambeth Council to continue doing so) (see section 5.7 of this Policy for further details concerning the right to object);
4. The personal data has been processed unlawfully;
5. The personal data needs to be erased in order for Lambeth Council to comply with

a particular legal obligation**.**

Unless Lambeth Council has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed within one month of the request.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible to inform them or would require disproportionate effort to do so).

The right to erasure does not apply to the lawful bases for processing of legal obligation or public task.

5.5 The Right to Restrict Processing

Data subjects may request that Lambeth Council ceases processing the personal data it holds about them. If a data subject makes such a request, Lambeth Council shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible to inform them or would require disproportionate effort to do so).

5.6 The Right to Data Portability – (only applies to Consent and Contract Lawful Bases)

Where data subjects have given their consent to Lambeth Council to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between Lambeth Council and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed within one month of the request.

The right to data portability does not apply to the lawful bases for processing of legal obligation, vital interests, public task or legitimate interests.

5.7 The Right to Object

Data subjects have the right to object to Lambeth Council processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to Lambeth Council processing their personal data based on its legitimate interests, Lambeth Council shall cease such processing immediately, unless it can be demonstrated that Lambeth Council's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to Lambeth Council processing their personal data for direct marketing purposes, Lambeth Council shall cease such processing immediately.

Where a data subject objects to Lambeth Council processing their personal data for scientific and/or historical research and statistics purposes, the data subject must,

under the GDPR, "demonstrate grounds relating to his or her particular situation". Lambeth Council is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

The right to object does not apply to the lawful bases for processing of consent (instead data subject has the right to withdraw consent), **contract performance, legal obligation or vital interests**.

5.8 Automated Decision-Making and Profiling

Lambeth Council uses personal data in certain **automated decision-making** processes.

Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR and the DPA, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from Lambeth Council.

The right does not apply in the following circumstances:

1. The decision is necessary for the entry into, or performance of, a contract between Lambeth Council and the data subject;
2. The decision is authorised by law; or
3. The data subject has given their explicit consent.

Profiling

When personal data is used for profiling purposes, the following shall apply:

1. Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
2. Appropriate mathematical or statistical procedures shall be used;
3. Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
4. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

6. Organisational Measures

Lambeth Council shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, agents, contractors, or other parties working on behalf of Lambeth Council shall be made fully aware of both their individual responsibilities and Lambeth Council's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
2. Only employees, agents, sub-contractors, or other parties working on behalf of Lambeth Council that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Lambeth Council;
3. All employees, agents, contractors, or other parties working on behalf of Lambeth Council handling personal data will be appropriately trained to do so;
4. All employees, agents, contractors, or other parties working on behalf of Lambeth Council handling personal data will be appropriately supervised;
5. All employees, agents, contractors, or other parties working on behalf of Lambeth Council handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the

workplace or otherwise;

6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed by each service area;
7. All personal data held by Lambeth Council shall be reviewed periodically, as set out in Lambeth Council's Records Management and Retention Policy;
8. All employees, agents, contractors, or other parties working on behalf of Lambeth Council handling personal data will be bound to do so in accordance with the principles of the GDPR, the DPA and this Policy by contract;
9. All agents, contractors, or other parties working on behalf of Lambeth Council handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Lambeth Council arising out of this Policy, the GDPR, and the DPA; and
10. Where any agent, contractor or other party working on behalf of Lambeth Council handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Lambeth Council against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

7. Transferring Personal Data to a Country Outside the EEA

Lambeth Council may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
3. The transfer is made with the informed consent of the relevant data subject(s);
4. The transfer is necessary for the performance of a contract between the data subject and Lambeth Council (or for pre-contractual steps taken at the request of the data subject);
5. The transfer is necessary for important public interest reasons;
6. The transfer is necessary for the conduct of legal claims;
7. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
8. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

APPENDIX A – Privacy Notice Procedure

1 INTRODUCTION

2 PRIVACY NOTICE PROCEDURE

2.1 DOES THE DATA SUBJECT ALREADY HAVE THE INFORMATION?
2.2 PRIVACY NOTICE PROVIDED TO DATA SUBJECT AT THE TIME OF COLLECTION
2.3 INFORMING THE DATA SUBJECT
2.4 FURTHER PROCESSING

3 'LAYERED' PRIVACY NOTICE EXAMPLE

1. INTRODUCTION

This procedure is intended to be used when a new or changed process is put in place which requires the collection of personal data from data subjects who fall within the scope of the GDPR and the DPA.

The GDPR, mainly in articles 13 and 14, requires that specific information is provided at the point of data collection or receipt which informs the data subject about the use that the data will be put to, and their rights over that data. This information will vary according to the specific circumstances and this procedure should be used to ensure that the correct information is given in the correct format so that Lambeth Council remains compliant with the GDPR and the DPA at all times.

Whereas in the past, information regarding privacy has tended to be provided in a single document (often called a "Privacy Policy"), the GDPR lends itself more to an approach where individual privacy notices are used according to the transaction or service involved. For example, one privacy notice may be displayed for a Council service on our website, and a different privacy notice is displayed when an individual signs up to receive a newsletter from the Council or fills out a paper form. This allows the privacy information provided to be more transparent and less confusing for the data subject.

Such privacy notices may be used in conjunction with a more traditional privacy policy if desired by providing a link to further and more detailed information (see 'layered' privacy notice example in section 3 of this procedure).

This procedure should be considered in conjunction with the following related documents:

- *Data Protection Policy*
- *Legitimate Interest Assessment Procedure*

2. PRIVACY NOTICE PROCEDURE

The purpose of this procedure is to create an appropriate privacy notice which provides the data subject with the information they are required to receive, in as fair and transparent a way as possible.

The GDPR specifies the information that must be provided to the data subject. This procedure describes that information and explains how to create a privacy notice that meets the requirements.

APPENDIX A

2.1 Does the data subject already have the information?

The GDPR requires the data subject to be provided with the listed information ***unless the data subject already has the information***. It is therefore important to determine whether it is reasonable to believe that the data subject is already aware of all of the information that would otherwise be required to be provided (i.e. if the data subject has already been provided with a privacy notice by Lambeth or a 3rd party explaining how Lambeth will use their personal data).

Where this is the case, the rationale for this belief must be documented and retained as evidence of GDPR compliance. Care should be taken to ensure that this applies to **all** of the information required and **all** of the data subjects affected, otherwise steps should be taken to address any gaps.

2.2 Privacy notice provided to the data subject at the time of collection

In the event that the data subject does not have the information required, the following must be provided at the time when personal data are obtained:

1. Identity and contact details of the controller (Lambeth Council) and of the controller's Data Protection Officer (DPO)
2. The purposes and legal/lawful basis of the processing (e.g. consent, legal obligation, legitimate interest)
3. The legitimate interests pursued by the controller, or by a third party (if legitimate interest is defined as the lawful basis of the processing)
4. The recipients, or categories of recipients, of the data, if any
5. Details of any planned transfers of personal data to a third country or international organisation
6. The retention period or length of time that the personal data will be stored for (or the criteria used to determine that period)
7. The data subject's rights to access, rectification, erasure and portability of the personal data (depending on the lawful basis used, see below)
8. The data subject's rights to restriction of, or objection to, processing of their personal data
9. The data subject's rights to withdraw consent at any time (if consent is used as the lawful basis of the processing)
10. The data subject's right to lodge a complaint with the ICO
11. Whether the collection of the personal data is a statutory or contractual requirement and whether they are obliged to provide it (if the lawful basis is legal obligation or contract performance) and the consequences of not providing it
12. Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved

Care must be taken to explain the data subject's rights in the context of the lawful basis of the processing. For example, if the lawful basis is contractual then the right to withdraw consent does not apply; or if the lawful basis is 'public task' then the right to erasure (right to be forgotten) does not apply.

APPENDIX A

2.3 Informing the Data Subject

As with all information provided to data subjects in accordance with the GDPR, the information must be in an intelligible and easily-accessible form, using clear and plain language. The best method of providing the information to the data subject will depend upon the specifics of the business process and may include one or more of:

• As a notice on a website • As a notice on a form • Via email	• Via physical post • By telephone • Face to face

The approach to privacy notices needs to be carefully planned so that the relevant information is presented to the data subject at the appropriate time. This will tend to mean that a coherent set of privacy notices is required, rather than a single document that covers all processing. Each privacy notice should be designed to be displayed at the appropriate point in the process (generally the point of collection of personal data) and be specific to the information being collected, the purpose for which it will be put and the lawful basis of the processing involved. This is often referred to as a “just in time approach” to privacy notices.

Equally, the best way to present the information should be carefully considered. Presenting a link to other sections of the relevant privacy notice may meet the requirements of GDPR on a website, but alternative methods of design (i.e. for paper forms) may allow a smoother user experience. (For questions regarding your privacy notice or to have your privacy notice(s) reviewed, please contact the Information Governance Team).

2.4 Further Processing

However it is obtained, if it is decided to use the personal data for a purpose other than that for which the data were obtained or collected, further information about that purpose, and the basis on which it is deemed lawful, must be provided to the data subject before the processing happens.

APPENDIX A

3. 'LAYERED' PRIVACY NOTICE EXAMPLE

NAME OF SERVICE / TEAM OR PROCESS (i.e. Parking and Enforcement, Council Tax)

Controller DPO

Email infogov@lambeth.gov.uk
Address: London Borough of Lambeth, Head of Information Governance, PO Box 734, Winchester, S023 5DG
Telephone: 020 7926 7717

Information we collect

Name
Email Address
Telephone Number
Postal Address
Bank/Payment Information (where applicable)
Agent contact details (if applicable)
Enforcement Investigation

Purpose

Service Delivery
Public Records

Lawful Basis

Legal Obligation (provide applicable statutory authority)

Recipients

Other local agencies
Police
Fire Brigade
Government agencies and / or statutory consultees
Third party contractors related specifically to planning and building control applications
And where authorised by legislation, the general public.

Rights

You have the right to access, rectify and delete personal information, in addition to other rights as explained in the full version of our privacy notice.

You have the right to contact us with a complaint if you're unhappy with the way your personal data has been used.

We are committed to resolving complaints about our collection or use of personal information.

You also have the right to lodge a complaint with the ICO if this issue is not resolved. You may at any time control access to and use of your personal information by contacting the Controller DPO.

Such control will include the ability to see what information we hold and to opt out of any use of your personal information and to prevent disclosure to any third party except as required by law or the order of a court of proper jurisdiction.

Additional Information

To see a full version of our privacy notice, please visit: lambeth.gov.uk/privacy-notice

APPENDIX B

REPORT A DATA BREACH TO LAMBETH COUNCIL

If you believe there has been a data breach, raise the incident immediately by calling 24/7 dedicated line 0207 926 9111 and provide as much information as possible from section 2.1 (see bullet points below) of the Personal Data Breach Notification Policy & Procedure. This will serve both internal staff and business partners and ensure the incident is responded to immediately.

If unable to get through the phone line, send an email providing the same information to Infogov@lambeth.gov.uk with "POTENTIAL DATA BREACH" as the subject line.
When reporting a data breach, please provide the information below to the extent known:

- The date and time that the breach was discovered
- The date and time that the breach is believed to have occurred
- The data items included (i.e. names, addresses, bank details, biometrics)
- The volume of data involved
- The categories and number of data subjects affected
- The nature of the breach (i.e. theft, accidental destruction, disclosure)
- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The actions that have been taken to manage the impact of the breach
- Contact details of the person handling the breach within our organisation
- Any other factors that are deemed to be relevant

APPENDIX C

Article: Consent to Direct Marketing under the GDPR
Rosalee Dorfman Mohajer (Pupil Barrister at Lambeth Council)
20 May 2018

Have you been receiving emails about the General Data Protection Regulation (GDPR) asking you to renew your consent to keep in touch? In some cases they may not be necessary if the original consent met the GDPR requirements. This article clarifies what consent means in the GDPR and for Lambeth Council and direct marketing.

First, you should consider whether you need to ask for someone's consent to process their personal data. Consent is one of the six lawful bases to process personal data in the GDPR. If you rely on another lawful basis you will likely not need to be concerned with consent and should not rely on consent as it would present a false choice. Most communication Lambeth Council has with individuals would fall within another lawful purpose, i.e. the processing is necessary to carry out a task in the public interest or an official function vested in the local authority. Lambeth Council should not require someone to agree to process their personal data as a condition of service, as consent is unlikely to be the appropriate basis in that context and in some cases would be invalid. For example, if a café asks to collect your personal data for direct marketing in return for using their free wifi, your consent would be invalid because the processing is not necessary for the provision of the wifi service. When Lambeth Council use direct marketing, website cookies or other online tracking methods, consent will likely be the applicable basis.

Second, you need to ask whether the consent valid. The definition of consent is (GDPR Article 4(11)):

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The difference between the previous definition in the Data Protection Act 1998 and the current definition of consent is that there must be an affirmative action and the indication must be unambiguous. In addition the data controller (Lambeth Council) needs to inform the individual that they can withdraw consent without detriment and has the right to object to the processing of their personal data for the purposes of direct marketing. In summary, the Information Commissioner's Office (ICO) Guidance on Consent clarifies that the GDPR requires that consent be:

- Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
- Active opt-in: pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (eg a binary choice given equal prominence).
- Granular: give distinct options to consent separately to different types of processing wherever appropriate.
- Named: name your organisation and any other third party controllers who will be relying on the consent. If you are relying on consent obtained by someone else, ensure that you were specifically named in the consent request – categories of third-party organisations will not be enough to give valid consent under the GDPR.
- Documented: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented. You need to have proof that the individual consented.
- Easy-to-access ways to withdraw consent: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you need to have simple and effective withdrawal mechanisms in place.
- No imbalance in the relationship: consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis where possible.

As mentioned in the last bullet point above, public authorities are unlikely to be able to rely on consent for data processing because usually there is a clear imbalance of power and the consent is not “freely given”. However, direct marketing is an exception because the usual imbalance does not exist where the local authority is marketing, for example a venue.

If the original consent fit the above requirements then it is valid and the individuals do not need to renew their consent. If individuals have indicated that they *do not* wish to be contacted, the local authority cannot contact them if they only lawful basis is consent (this recently happened in a case involving Honda).

Third, if the communication is direct marketing, obtaining consent of the individual is necessary to process their data. Direct marketing is the communication of any advertising or marketing material which is directed to particular individuals (Data Protection Act 1998, s 11(3)). This covers the promotion of aims and ideals as well as the sale of products and services but the regulation is limited to unsolicited marketing, meaning that it has not specifically been asked for. It extends to not-for-profit organisations (Direct Marketing ICO Guidance, p. 5).

Since 2003 direct marketing has relied on consent. The Privacy and Electronic Communications (EC Directive) Regulation 2003 (PECR) both adopts the definition of consent in the Data Protection Act 1998 and introduced a tighter requirement that you can

only send an electronic marketing message when the individual has consented to receive it from the sending organisation or there is an existing customer relationship and have offered them the opportunity to opt out. Consent lasts only as long as the circumstances remain the same and the consent must be specific to the type of communication in question.[1] The restriction is similar to what is now required by the GDPR. Hence, a recent article in Wired stated that, because of the existing requirements in PECR, companies may not have needed to send out the emails asking for renewal of consent, because people either have already consented (to the GDPR standard) or are receiving them to business email addresses, for which consent to receive them may not be needed.

In conclusion, you should consider (i) whether you need to ask for someone's consent to process their personal data, (ii) if so, is the consent you are seeking valid and (iii) if you are engaging in direct marketing, was the original consent GDPR-compliant. If the original consent was GDPR-compliant then you do not need to ask for a renewal of consent after the GDPR comes into effect on 25th May 2018.

For further information please see the following resources:

- EC Article 29 Working Group Guidance on Consent
- Information Commissioner's Office Guidance on Consent (GDPR)
- ICO Direct Marketing Guidance (contains GDPR updates)

If you have any questions about the article please contact Matthew Ginn or Rosalee Dorfman Mohajer.

[1] PECR added the requirement that consent for electronic marketing calls or messages that: "the [recipient] has previously notified [the caller or sender] that he consents for the time being to such communications being sent by, or at the instigation of, the [caller or sender]" (Regulation 21 and 22).

APPENDIX D – LEGITIMATE INTERESTS ASSESSMENT PROCEDURE

Sample LIA template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
Reasonable expectations
• Do you have an existing relationship with the individual? • What's the nature of the relationship and how have you used data in the past? • Did you collect the data directly from the individual? What did you tell them at the time? • If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? • How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? • Is your intended purpose and method widely understood? • Are you intending to do anything new or innovative? • Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation? • Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
Likely impact
• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their personal data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would you be happy to explain the processing to individuals?

• Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	
LIA completed by	
Date	

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.