Data Protection Policy

1. Purpose and Scope

The policy sets out how Homes for Lambeth Group Ltd and its subsidiaries ("HFL") will comply with the Data Protection Act 2018 ("DPA") and associated legislation including the EU General Data Protection Regulations 2016 ("GDPR").

This policy applies to all staff of HFL including permanent, temporary, contract, secondees, work experience staff, board members and independent committee members who may be involved in the processing of personal information on behalf of HFL and extends to data that is held on paper or electronically. Where HFL engages the service providers to deliver a service, such as housing management contractors, construction contractors and development management teams, this policy is applicable.

HFL holds information about residents, prospective residents, those it is engaging with around future developments, stakeholders, staff and other individuals who may contact the organisation. It is therefore important that HFL strikes a balance between the fundamental right to privacy and a private life and its legitimate interests in delivering services which rely on using personal and data including responses to surveys and feedback requests etc. (hereafter referred to collectively as "data"). Many staff members and contractors require access to the personal data of others in order to effectively fulfil their role. HFL is committed to protecting the information rights of both its staff and customers. HFL is committed to updating all staff and customers of any changes to the use of their information and or material updates to this policy.

2. Objectives

The objectives of this policy are:

- to comply with the DPA and GDPR while delivering effective and efficient services
- to outline, guide and monitor the coordination of the information, security and data handling procedures in force within HFL
- to promote confidence in HFL's information, security and data handling procedures
- to provide assurances to residents about how their data will be processed and stored
- to provide assurances for third parties dealing with HFL
- to provide a benchmark for employees on information, security, confidentiality and data protection issues.

In order to support these objectives, HFL will:

- ensure that all activities that relate to the processing of data have appropriate safeguards and controls in place to ensure information, security and compliance
- ensure that all HFL staff including interims and secondees are operating under agreements that make reference to compliance with the relevant legislation
- ensure that contractors acting on behalf of HFL are given access to personal information that is appropriate to the duties they are undertaking and no more
- ensure that HFL staff including interims and secondees and Board members understand their responsibilities regarding data protection and information security under the relevant legislation, and are provided with training. Recording this in a centrally update database, which is updated in inductions to HFL
- ensure that all contracts with third parties, where data is processed and / or shared, make reference to compliance with the relevant legislation and how data will be managed in a compliant manner, including copies of the organisation's data protection policy. Where HFL shares data with third parties, this will be limited to the information required to perform their duties under the contract.

3. Roles and Responsibilities

All staff at HFL have a responsibility to observe and understand the data protection principles in this policy. There are a number of senior roles within HFL that have key data protection responsibilities, including:

Executive Directors (ED)
Executive Directors 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.

Information Asset Owners (IAO)
IAOs are 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. Record management is a key responsibility of an IAO.

Information Asset Administrators (IAA)
IAAs have day to day responsibility for record management for their information assets and ensure that all data protection principles and this policy are fully observed and applied by staff in their operational area. IAAs will be responsible for handling, coordinating and responding to Subject Access Requests for their specialist area.

Data Protection Officer (DPO)
The DPO will be part of the scope of the Operations Director 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 Information Commissioner's Office (ICO).

4. Data Protection Principles

HFL staff must ensure that all data it collects, processes and stores is done so in compliance with the DPA and GDPR. This means that all 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
- 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[1]
- processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures
- consideration and adherence to the Cyber Security protocols and take every possible step to protect all data from external hacks and malicious attacks.

[1] Data may be stored for longer periods if it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementing appropriate measures required by the GDPR to safeguard the rights and freedoms of the data subject.

HFL is required to explain to all individuals how they will use personal data which is collected and shared. Privacy Notices must be provided prior to any personal data processing activity.
HFL staff must consult the HFL guidance and procedures for managing data before processing it. The guidance will include checklists to assist staff to ensure data is processed in a compliant manner.

5. Data Security

All HFL representatives processing data on HFL's behalf will be appropriately trained and must understand that they are contractually responsible for following good data protection practice. Each individual is responsible for ensuring that they receive this training and that they have read and understood the relevant policies.

Methods of processing personal information will be clearly communicated within HFL and regularly reviewed. Access to HFL's different systems will be password protected to ensure that personal information is only accessible by those individuals that need it to undertake their job. Paper files and manual records containing personal data will be stored in secure environments. A master record of what information types and classes are kept forms part of HFLs Quality Management System.

All reasonable steps will be taken to ensure that any data processor that HFL uses has appropriate technical and organisational security measures in place to safeguard personal data. HFL must request data protection policies from third parties at their tender stage and other assurances as required for the scope of the processing.

6. Data Sharing

There are a number of occasions where it will be necessary for HFL to share data collected with third parties. For example, tenant data will be shared with and / or disclosed to housing management contractors that may be appointed from time to time to deliver services on behalf of HFL Homes. Personal information will also be shared with Lambeth Council when providing housing to referrals from their local housing list or particular schemes. Access to data will also be provided to those engagement partners who are supporting resident engagement around the design of their future estates. Data may also need to be shared for other purposes beyond these examples.

If HFL shares personal data on a regular basis with other organisations we will ensure that there are written protocols in place governing the sharing of that personal data. For example, in relation to tenant data, tenants will be told:

- who we are;
- why we are going to share personal data;
- the type of organisation(s) we are going to share it with; and
- further information of the situation where the nature of the sharing is such that some aspects of it would not be in the "reasonable expectations" of the individual that we would use their data in that way in order to allow the sharing to be considered fair.

When a request for disclosure is made by an organisation, HFL will consider each request individually and where a disclosure takes place, HFL will disclose only the minimum amount necessary.

HFL reserves the right to disclose information under certain circumstances where allowed by law.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the requirements in Appendix A applies.

7. Rights of Data Subjects

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

i. The Right to be Informed
ii. The Right of Access
iii. The Right to Rectification
iv. The Right to Erasure ('Right to be Forgotten')
v. The Right to Restrict Processing
vi. The Right to Data Portability
vii. The Right to Object
viii. Automated Decision-Making and Profiling Rights

Such a request from a data subject should be submitted to the DPO at the contact details below.

8. Data Retention

HFL will only retain personal data for the length of time necessary to perform the process for which it was collected. This applies to both electronic and non-electronic data. This will be assessed on an annual basis with the headline results reported to the Board. Considerations for whether data needs to be retained include any legal requirements that apply for the retention of any particular data e.g. Employment law, Landlord, Health & Safety and Tenant law, Regulation. In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing, after which is must be disposed and erased carefully.

Individuals can request deletion of certain types of information about them where one of a number of circumstances apply:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation

9. Complaints, enforcement and dealing with breaches

Complaints regarding data protection and the handling of Subject Access Requests should be passed to the DPO.

Any HFL employee, contractor or Board member who suspects that a data breach has occurred or will occur, must report it to the DPO immediately (contactable below). Suspected breach will be then handled according to HFLs data breach policy.

All HFL employees, contractors and Board members are expected to co-operate in full with any investigation undertaken by (or on behalf of) the DPO or other representatives undertaking an investigation on behalf of the DPO.

HFL's DPO can be contacted at:

Data Protection Officer
Homes for Lambeth
Civic Centre
6 Brixton Hill Brixton
London SW2 1EG
foi@homesforlambeth.co.uk
020 7926 9056

10. Policy Review

This policy will be reviewed at least every three years. However, we will monitor its effectiveness on an ongoing basis to ensure that it is fit for purpose and always displaying best practice.

HFL Policy Name:	**HFL Data Protection Policy**
HFL Policy Owner:	HFL Operations Director (Interim Financial Director until Operations Manager is in post)
Applies to:	All HFL Group Companies
Policy Compliance:	Annual Review
Policy Review Cycle:	Every 3 Years (min or as per legal/regulatory requirements) Next review Jan 2022
Version Control/Audit Trail:	
	DRAFT 1.0 Prepared for HFL Board approval Jan 2019. Based on Lambeth Council policy and policy examples from other organisations in the sector. The material changes from the Lambeth Council policy are: • More detail on roles and responsibilities • Reference to HFL roles that do not reflect the Council structure.
Version 1	Approved by HFL Board/s January 2019

Appendix A: Transfers of Personal Data Outside 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.