Data protection policy

1.0 Purpose and Scope

The policy sets out how Notting Hill Genesis (NHG) will comply with the Data Protection Act 1998 and associated legislation including the EU General Data Protection Regulations 2016. It applies to all personal data processed by NHG and its contractors. It forms part of the Information Management suite of policies.

This Policy applies to all staff of NHG. This includes permanent, temporary, contract, work-experience staff, volunteers, board members and independent committee members who may be involved in the processing of personal information on behalf of NHG and extends to data that is held on paper or electronically.

NHG holds information about customers, staff and other individuals who may contact the organisation. It is therefore important that NHG 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 data. Many staff members require access to the personal data of others in order to effectively fulfil their role. NHG is committed to protecting the information rights of both its staff and customers.

The obligations on NHG with regard to personal information are set out in the Data Protection Act 1998, the General Data Protection Regulations and associated legislation. This policy sets out the principles NHG adheres to in regard to personal data, as well as demonstrating its commitment to comply with the relevant legislation.

2.0 Definitions

Key terms referred to in the policy are explained below. For a detailed glossary of terms contained in the Data Protection Act, please refer to the ICO website (see Reference for details).

Data protection term	Definition
Confidentiality	One of the key components of information security so that information is only shared with authorised individuals
Data Breach	Is an incident in which personal/sensitive or confidential data has potentially been viewed, stolen or used by an individual without authorisation.
Data Protection Officer	Nominated member of staff with responsibility for monitoring compliance with the Data Protection Act and associated legislation.

Data Inventory	A recording system for identifying, mapping and documenting key information assets within an organisation, which contain personal data, and sets out the ownership, security, classification, location and data sharing elements. Used to assess risk in relation to information and ensure adequate controls are in place based on the specific requirements of the asset e.g. encryption
Fair Processing Notice (FPN)/ Privacy Notice	When personal data is collected from an individual, they must receive an explanation as to what personal data is to be collected, why and the reasons for its retention.
Information Commissioners Office (ICO)	The UK's regulator for Data Protection. They handle the registration of organisations, queries, investigation and can administer fines.
Integrity	One of the key components of data security, ensuring that data remains accurate and trustworthy and provides assurance that it has not been altered or otherwise tampered with.
Personal data/ Personal Identifiable Information (PII)	Any information which directly or indirectly denies a living individual, including any identifier such as NI number, IP Address, NHS number. Can also fall into special categories / sensitive personal data (e.g. ethnicity, disability, sexual orientation), which requires additional protections when processed such as explicit consent to collect.
Sensitive data/ special category data	Personal data consisting of information such as: racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life. GDPR extends this to include genetic and biometric data for uniquely identifying a natural person. Criminal Data is covered under Article 10 of the GDPR>
Processing of data	Any action involving data including collection, using, disclosure, creation, retention, sharing, disposal or storage of personal data.

*For the purpose of this policy when 'personal data' is used it will refer to personal, sensitive and special categories of data.

3.0 Policy Statement

This Policy sets out how NHG complies with the Regulations and Data Protection principles to:

- Take a privacy by design approach to the processing of personal information using Privacy Impact Assessments
- Ensure that all personal data or personally identifiable information is processed in accordance with the privacy expectations of the individuals whose data we hold (including staff),
- Process personal data lawfully and identify the legal basis for processing
- Process information fairly and in a transparent manner by telling those individuals whose data we process, how we intend to use their information in a way that is understandable to them through relevant and timely privacy notices
- Only collect personally identifiable information for specified, explicit and legitimate purposes (purpose limitation)
- Ensure that the information we use is accurate and where necessary kept up to date (accuracy)

- Not store personally identifiable information for any longer than is necessary for the purpose for which it was collected (storage limitation)
- Personal data will only be processed in a way that ensure appropriate security, using appropriate technical and organisational measures (integrity and confidentiality)
- Ensure that individuals can access their rights in respect of the information we process about them, including the right of access, right to be forgotten, right to object and right of restriction.
- Maintain all necessary records to maintain compliance and demonstrate accountability with the obligations on it.

4.0 Privacy by Design / Privacy by Default

NHG will take a privacy by design/ default approach of personal data, ensuring that all personal data is processed in a way which respects the privacy of the individuals whose data we process

4.1 Internal & External Privacy Notices

NHG will issue Privacy Notices explaining in plain English how it intends to use information at the time of collection, or as soon as possible thereafter.

4.2 Consent

NHG will identify the most appropriate legal basis for processing personal data and will explain this at the time the data is collected. Where the legal basis for processing is consent, NHG will record the specific consent, and give individuals the option to withdraw their consent.

4.3 Privacy Impact Assessments

NHG will carry out Privacy Impact Assessments to identify and manage any risks to the privacy of individuals, prior to the start of any new process or change to processing of personal data. The Data Protection Officer will be consulted on the privacy impact assessments. Consultation may be carried out with customers and individuals whose personal data may be impacted by the processing prior to the project being carried out. Where the risks are significant, advice will be sought for the Information Commissioner as the supervisory authority for the UK.

5.0 Roles and Responsibilities

5.1 Data Protection Officer

NHG processes significant amounts of personal data of a large number of individuals and also undertakes surveillance through the use of CCTV cameras of public spaces.

The Company Secretary is designated 'Data Protection Officer' and has ultimate responsibility for data protection within NHG as follows:

- Informing the organisation of their obligations pursuant to the relevant legislation (see Background Legislation for details)
- Cooperating with the Information Commissioner's Office

Regular checking and monitoring that NHG is compliant is led by the Data Compliance and GDPR Programme Team and Data Protection Officer, within their legal obligations under the GDPR, who will be responsible for:

- Providing advice and assistance to staff on the application of the Data Protection Act.
- Monitoring compliance with the regulation including training, awareness-raising and audits.
- Providing assistance with the completion of Privacy Impact Assessments
- Acting as point of contact for the Information Commissioner and data subjects wishing to exercise their rights under the Data Protection Act.

5.2 Staff

Compliance with data protection legislation and internal policy is the responsibility of all employees. NHG will ensure that all staff will:

- Complete the mandatory data protection training and any other data protection training as required
- Store personal information in appropriate, suitably secure access-controlled locations, in accordance with the IT Security policy
- Ensure that confidentiality of any folders and files, both hard copies and electronic, that they are using when working from home both in transit and at rest are secure e.g. lockable cabinets at home, not using public wifi without connecting through VPN eg Citrix.
- Use private areas where data cannot be overlooked when working on sensitive material
- Lock away sensitive or personal information during breaks
- Avoid leaving personal information unattended for example at desk or the printer
- Ensure when sending personal information outside of the organisation that such files are sent securely.
- Not send any personally identifiable information about customers or suppliers or other staff to unauthorised personal email accounts (e.g. staff personal accounts, family members etc.). Staff may send their own personal data e.g. payslips to their own personal accounts for their own use. Only NHG approved devices and services must be used for accessing information.
- Comply with the requirements of the IT Security policy and the Clear Desk / Screen policies
- Dispose of information in a secure manner once it is no longer required in line with the Records Management policies and associated retention schedules.

5.3 Accountability

NHG will ensure that all relevant records are maintained in order to demonstrate compliance with the principles of the Act. The Data Inventory will be owned and maintained by the Data Protection Officer. Records of consent will be recorded against the appropriate individuals' records in the relevant corporate record system.

6.0 Storage and Security

6.1 Secure Storage

All personally identifiable information must be stored securely in line with the Information Security Management System requirements.

6.2 Data Disposal

Where there is no longer a legitimate basis to process the information, staff will dispose of it in a secure manner. Details of how long information must be retained for are set out in the Records Management policies and retention schedules.

6.3 Incident/ Breach Management

Where there has been a suspected breach of the Data Protection Act and GDPR in relation to personal information including unauthorised access, loss, or alteration, it must be dealt with in accordance with the Information Security Incident Procedure.

All incidents involving personal data will be classified as a P1 / P2 incident under the Procedure.

The Data Protection Officer must also be informed, and where there is significant risk to the privacy of the data subject(s) a notification made to the ICO and the data subject rights within 72 hours of NHG becoming aware that personal data has been compromised.

6.4 Rights of Individuals

Individuals have the following rights under the Act and GDPR:

Right to be informed	The right to be informed at the time the data is collected of how the data will be used
Right of Access by Data Subject	The right to receive a copy of the information held by NHG
Right of Rectification	The right to correct any inaccurate information, including by means of a supplementary statement
Right to Erasure (right to be forgotten)	The right to have personal data deleted where one of the following conditions applies: • Information is no longer necessary in relation to the purposes for which they were collected • Consent is withdrawn (where consent was legal basis for processing) • Objection received and no legitimate grounds to continue processing • Processing is unlawful • Data have to be erased for compliance with other legal obligation
Right to Restriction	Right to have processing of personal data restricted in certain circumstances
Right to Data Portability	Right to receive information in a machine-readable format and transmit it to another data controller
Right to Object	Right to object to processing on the basis of the individual's circumstances at the time of processing, to any processing on the basis of the performance of the public task, or legitimate interests of the data controller or third party.
Automated processing and decision making including profiling	Right to not be the subject to a decision based solely on automated processing (i.e. without human intervention), including profiling, which would produce legal or similarly significant effects on the individual.

Any request must be passed to the Data Protection Officer as soon as it is received to ensure that is it processed appropriately and within the relevant timescale, i.e. one calendar month.

7.0 Research Using Personal Data

NHG carries out a large amount of research in order to support and improve the services we provide to our customers. Personal data processed for research purposes must not be used to support decisions with respect to individual customers or processed so as to cause them substantial damage or distress. Such information is exempt from the right of subject access as long as the results of the research do not identify individuals.

NHG will ensure that staff using personal data in research:

- Understand how personal data may be used in research
- Use the minimum data necessary for the research, including, wherever possible, anonymised data
- Ensure their processing complies with all the data protection principles
- Seek advice from the Head of Policy and Performance and the Data Protection Officer before processing of personal data begins
- Where relevant, inform data subjects about the purposes of the processing and ensure valid written consent is obtained
- Ensure all personal data collected are necessary for the purpose(s) of the research
- Keep the data securely.

8.0 Third Party Contracts and Data Sharing

Contracts, data sharing agreements and other information sharing protocols with agents, subcontractors, Local Authorities, user-referral agencies or other agencies (such as the police or probation authorities) that require the sharing of personal information must include suitable clauses with regards to confidentiality and non-disclosure and include reference to the Data Protection Act and GDPR.

It is important also that the sharing of personal information supports the purpose for which it was provided. Sharing of information beyond the scope of that authority is unlawful.

All data sharing agreements must be signed off by the Data Protection Officer and relevant Director. All contracts must include standard data protection clauses, and be approved by the Procurement Team. Further detail on Information Sharing is set out in the Information Sharing Policy.

9.0 Breaches of this Policy

Any member of staff who considers that this policy has not been followed in respect of personal data about themselves or others should raise the matter with their line manager and the Data Protection Officer.

Any breach or suspected breach of this policy will be investigated fully and the necessary remedial action taken. Such action must involve a decision as to whether or not to voluntarily notify the Information Commissioner's Office of any breach of the Data Protection Act and

GDPR. The decision on whether to contact the ICO will be taken by the Data Protection Officer (in conjunction with the data team or the Director in more serious cases).

Serious breaches of this policy may result in disciplinary action or, in severe cases, criminal prosecution against individuals.

10.0 Complaints

Where an individual is unhappy with the processing of their personal data, they have the right to complain to the Data Protection Officer and to the Information Commissioner's Office.

Complaints to the Data Protection Officer will be dealt with in line with the existing NHG Complaints Procedure, with relevant input from the Data Protection Officer.

Any complaints from the Information Commissioner will be dealt with directly by the Data Protection Officer and NHG will fully cooperate with any investigation proceedings.

NHG will ensure that the findings from any complaints are used to drive an improved service for the customer.

11.0 Data Protection Queries

Frontline staffs, i.e. Housing/ Property Management Officers, are responsible for dealing with queries. Advice and support will be set out in our procedures.

12.0 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.

13.0 Our approach

In writing this policy we have carried out a diversity and inclusion impact assessment and no adverse impacts were identified. The policy does not involve the use of personal, sensitive information so it has not been necessary to carry out a privacy impact assessment.

14.0 Reference

Key legislation

- Data Protection Act 1998
- Data Protection Act 2017 (currently draft)
- General Data Protection Regulations (EU Regulation 2016/679)

Document control

Author	Catherine Preston and Emma Turay
Approval date	26 March 2018
Effective date	4 April 2018
Approved by	Day 1 Policy Approval group
Policy owner	Company Secretary
Accountable Director	Group Director of Central Services

Version control

Date	Amendment	Version
April 2018	New NHG policy created.	1.0

Appendix

Notting Hill is made up of multiple subsidiaries (detailed below) which sit under the Group name of NHG. They are each registered with the ICO and further registration details on each of them can be found via the links below or by searching with the registration numbers.

Legal entity	Registration number
Notting Hill Housing Trust	Z5766997
Notting Hill Home Ownership Limited	Z5501369
Folio London Limited	**Z9928895**
Arawak Developments Limited	**ZA099928**
Canonbury Developments Limited	**Z9928850**
Chobham Farm North LLP	**ZA093807**
Coat Wharf Limited	**Z3096019**
Grange Walk Notting Hill Limited	**Z309581X**
Great Eastern Homes LLP	**Z1656163**
Great Eastern Quay Limited	**ZA099961**
Notting Hill Commercial Properties Limited	**Z8743472**
Notting Hill Developments Limited	**Z1656194**
Notting Hill Home Options Limited	**Z2593237**
Presentation Market Rent Limited	**Z2593180**
Project Light (Market Rent) Limited	**ZA065332**
Project Light Development 1 Limited	**ZA065320**
Project Light Development 2 Limited	**ZA065326**
Seward Street Developments LLP	**Z2918400**
Touareg Trust	**Z9595710**