North Devon Homes
Group Data Protection Policy

Contents

Page Number

1. Policy

This policy sets out how North Devon Homes (NDH) will comply and work with data protection legislation and follow good practice to store and process data fairly and lawfully. This policy applies to NDH and all of its subsidiary companies.

2. Purpose

The purpose of this policy is to ensure that NDH complies with the seven key principles of the EU General Data Protection Regulation (GDPR) as outlined in 7.3.

The GDPR and the Data Protection Act 2018 regulate the processing of information relating to individuals. This includes obtaining, storing, using and disclosing such information. The legislation covers all data whether on paper, in computer files or recorded on other material. It also includes the recording and storage of digital images e.g. from Closed Circuit Television (CCTV) and cameras.

3. Scope

This policy applies throughout NDH and must be adhered to by all employees, Board Members, involved customers, contractors (whether working in NDH offices or its homes), consultants and any other person granted access to data held or processed by NDH.

Failure to comply with this policy may result in disciplinary action.

4. Responsibility

a. **The Board and Executive Team** are responsible for establishing and maintaining a control environment that promotes overall compliance. Approval of this policy and any significant amendments or updates made to it.

b. **All employees, involved residents, and Board Members** are responsible for ensuring, whilst undertaking their roles; they do so in compliance with this policy and the GDPR and Data Protection Act. They also have responsibility to report actual or potential data security breaches to the Information Security Compliance Group (ISCG) through their line manager or directly to a ISCG member.

c. The **Finance Director** is the appointed Data Protection Officer (DPO) and is responsible for tasks set out in Articles 38 (position of the DPO) and 39 (tasks of the DPO) of the GDPR to ensure that we remain compliant.

d. The **Finance Director** supported by ISCG members, is responsible for maintaining NDH's registration with the Information Commissioners Office (ICO) and for handling data protection questions from staff and all those covered under this policy. They shall also provide guidance on the GDPR, review and update policies and oversee requests from individuals to see the data held on them (subject access requests).

e. The **Information Services Manager** is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards, and ensuring that regular checks are performed through scans and penetration testing etc. to ensure security hardware and software is functioning properly. Evaluating any third party services the company is considering using to store or process data.

f. **HR Team**, along with the DPO, is responsible for the provision of adequate training.

g. **Heads of service and Line Managers** (as appropriate) are responsible for entries and amendments to the Information Asset Register. Also leading and fostering a culture that values, protects and uses data within the law for public good and know what data assets are held, who this data is shared with, know who has access and why, ensure that their use of the asset is monitored if required and identify any risks to the asset, and support risk management activity. They will ensure that their teams are regularly reviewing files held (hard and electronic) including archived files to implement secure disposal in line with the retention timescales applied.

h. **Line Managers** involved in procurement are responsible for ensuring that all contracts and tender documents are compliant with GDPR and the third party has adequate policy and procedures in place for GDPR. Advice should be sought from the Procurement Consultant as appropriate.

i. **The PR & Marketing Coordinator** is responsible for addressing any data protection queries from journalists or media outlets. Where necessary, ensuring that communications such as emails and letters contain the required Data Protection statement along with working with other staff to ensure promotional communications abide by data protection principles.

j. **Information Security Compliance Group (ISCG)** is responsible for monitoring and ensuring compliance in respect of:

i. Cyber attacks and data protection breaches (or near misses);

ii. GDPR compliance;

iii. GDPR Breaches and notification to ICO

iv. Rectifying actions for the above

v. Subject Access Requests

vi. Requests for erasure

vii. Maintenance of the Information asset register
viii. Data Protection Impact Assessments
ix. Identifying significant risks to the protection of personal data.

- The Group membership consists of the following posts:

a. Finance Director (who is also the DPO)
b. Heads of Asset Management, Housing and HR
c. IT Manager
d. Performance Improvement Manager
e. PR & Marketing CoOrdinator

It is the responsibility of all employees, Board members, consultants, contractor and sub-contractors (see Scope at paragraph 3), to maintain confidentiality and ensure they deliver their service in accordance with this policy.

A breach of data protection principles can be a serious offence and may lead to disciplinary action or even criminal prosecution. All employees should inform their line manager or another senior manager of any suspected breach of data protection principles or loss of data.

It is the responsibility of managers and heads of service to ensure that team members are following the Data Protection guidance and procedures. The DPO is responsible for ensuring overall compliance with this policy and the Data Protection Act and GDPR.

5. Principles

The following principles will apply to this policy, it will:

- comply with data protection law and follow good practice;
- protect the rights and freedoms of those whose personal data we use;
- be open, fair and transparent in the way we collect, use, share, store and delete personal data and,
- ensure that we have appropriate safeguards in place to minimise the risk of a data breach.

6. Review

This policy will be reviewed along with procedures and employees training needs at least once every two years, or earlier if necessary due to changes in legislation, to ensure that it continues to operate within best practice guidelines

The DPO will be responsible for ensuring that policy reviews are undertaken, that appropriate consultation takes place and that revisions are reported to the Board for its approval.

7. Application

The Executive Team will approve this policy and delegate responsibility to the DPO for ensuring that this policy is communicated and implemented.

The DPO will provide / arrange for training of employees to ensure that they fully understand the wider issues surrounding this policy and associated procedures. The Policy will be made available on the NDH intranet.

Training on this policy will be covered as part of the induction process for all new starters and GDPR e-learning module 1 will be mandatory for all staff.

Further in-depth training can be provided for employees who have extra responsibilities for data protection or who need extra clarification on what the Data Protection Act and GDPR means for them.

8. Legal framework

We are committed to ensuring that we comply with the requirements of the data protection laws in force in England and Wales including the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). We will also comply with any formal written guidance published by the Information Commissioner's Office (ICO).

The Data Protection legislation applies to personal data. Personal data is information from which a living individual either can, or potentially can, be identified. This applies to information about individuals which is in electronic form or in hard copy (where such information either is, or is intended to be, stored in a relevant filing system).

9. The Data Protection Principles

Under the GDPR there are 7 data protection principles (Article 5). The principles require those using personal to ensure that personal data is:

a. used in a way which it lawful, fair and transparent (the first data protection principle);

b. only collected for a specified, explicit and legitimate purpose (the second data protection principle);

c. adequate, relevant and limited to what is necessary for processing purpose (the third data protection principle);

d. accurate and up to date (the fourth data protection principle);

e. kept in a form which allows identification of individuals for no longer than necessary (the fifth data protection principle); and

f. kept appropriately safe against unauthorised processing, accidental loss, destruction or damage (the sixth data protection principle).

The Data Controller shall be responsible for, and be able to demonstrate compliance with the six principles above; this is deemed to be the seventh 'accountability' principle.

10. Lawful condition for processing

a. The first data protection principle requires us to ensure that we have a lawful basis for any processing of personal data. There are six lawful bases prescribed in Article 6 of the GDPR which are:

   a. the individual has provided their consent for us to use their data for a particular purpose; and
   b. our use of an individual's personal data is necessary in order for us to perform a contract between us and that individual.
   c. Processing is required for compliance with a legal obligation (e.g. verification of right to work in the UK)
   d. Processing is required to safeguard the vital interests of the Data Subject (e.g. medical emergency)
   e. Processing is required for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (e.g. in the case of local authority processing of Housing Benefit)
   f. Necessary for the purposes of legitimate interests pursued by the Controller or a third party, except where such interests are outweighed by the interests, rights or freedoms of the Data Subject.

b. Unless another lawful basis applies, we shall only use the personal data of a customer or an employee as is necessary for us to perform the contract between us and the customer or employee. Where the use of a person's personal data is necessary for us to perform a contract and that person, we do not also need their consent for such use.

c. Special categories of personal data (which were previously termed 'sensitive personal data'), includes information relation to a person's:

   - racial or ethnic origin;
   - political opinions;
   - religious beliefs / beliefs of a similar nature;
   - membership of a trade union;
   - physical or mental health; and
   - sexual orientation.

d. In order to lawfully use special categories of personal data, we must satisfy an additional lawful basis which is listed in Article 9 of the GDPR. These are:

   a. the individual has provided their explicit consent;

   b. processing is required for carrying out obligations under employment, social security or social protection law or a collective agreement (e.g. collection of equality data);

   c. processing is required to protect the vital interests of a Data Subject or another individual where the Data Subject is legally or physically unable to give consent

   d. processing carried out by a not-for-profit body with a philosophical, religious, political, or trade union aim, provided the processing relates only

to members or former members and provided there is no disclosure to a third party without consent.

e. Processing relates to personal date made public by the Data Subject

f. Processing is required for the establishment, exercise, or defence or legal claims or where courts are involved;

g. Processing is required for reasons of significant public interest

h. Processing is required for purposes of preventative or occupational medicine, for evaluating the working capacity of the employee, medical diagnosis, provision or management of health or social care systems or a contract with a health professional.

i. Processing is necessary for reasons of public health interest

j. Processing is required for archiving purposes in the public interest or historical and scientific research purposes.

e. The lawful basis on which we shall rely in relation to any particular categories of personal data and special categories of personal data shall be documented on our Information Asset Register.

f. We shall inform the individual of the lawful basis on which we shall rely through a privacy notice which has been made available to them.

11. Consent

NDH may process personal data and special category data for the purposes of satisfying operational and legal obligations such as the management of a tenancy, under lawful conditions for processing. Therefore NDH will rely on this as its lawful basis for processing and will not require consent to be obtained for its day to day operational management.

Should there be occasions where consent is the lawful basis for processing personal data, the consent must be freely given by the individual. The provision of consent cannot be a condition for us to provide a service to an individual that would not be freely given. Evidence of consent should be retained and where possible this should be in writing. Consent can be withdrawn at any time and this will be stated on the consent form as appropriate.

Consent under the GDPR must also be specific – we need to be clear in relation to what we are seeking consent for and it cannot be too wide-ranging. The individual must also take an active step to indicate that they are providing their consent - silence, pre ticked boxes or inactivity does not constitute consent.

12. Profiling

Data Subjects have a right to object to any automated decision if the decision results in legal effects or has a significant effect on the Data Subject. NDH will not carry out any activities that fall within the scope of 'profiling' as defined in GDPR. Should any activity arise that could be considered to be profiling, then consent for the activity needs to be obtained from the DPO prior to the activity taking place.

13. Direct Marketing Activities

No data will be processed for the purposes of direct marketing (unless explicit consent has been obtained). If a person feels that their data has been processed for direct marketing purposes, a complaint can be raised through the formal complaints process or directly to the DPO.

14. Individuals' Rights

Under the GDPR there are eight rights which individuals have over the use of their personal data. These are:

a. **The right to be informed:** Individuals have a right to be told how we use their personal data (see 14 below).

b. **The right of access:** individuals have a right to access their personal data which we hold (see 12 below).

c. **The right to rectification:** Where personal data is inaccurate or incomplete, an individual has the right to have that data rectified.

d. **The right to erasure:** In certain circumstances, an individual can ask that we delete their personal data (see 13 below)

e. **The right to restrict processing:** Individuals can limit our use of their personal data in certain circumstances.

f. **The right to data portability:** In certain circumstances, individuals can request that we provide their personal data in a way which can easily be reused by them or other service providers.

g. **The right to object:** Individuals can, in certain circumstances, object to our use of their personal data.

h. **The right not to be subject of automated decision:** Individuals can insist that they are not the subject of an automated decision concerning them.

15. Rights to access of information (subject access requests)

All individuals (employees, Board Members, customers, and suppliers etc) whose personal data is held by NDH have the right to request access to personal

information that we hold about them (a subject access request). There are limits to this right such as where the disclosure of such information would unreasonably infringe the data protection rights of a third party.

NDH must provide the information within one calendar month of receiving the request. Requests shall be overseen by the DPO in accordance with the subject access request procedure.

16. Right to erasure

A Data Subject may request that any information held on them is deleted or removed and any third parties who process or use data must also comply with the request.

The right to erasure only applies in specific circumstances which include:

a. If the personal data is no longer necessary in relation to the purpose for which it was collected;

b. We are relying on the individual's consent as the lawful basis for processing personal data;

c. We are relying on a legitimate interest as the lawful basis for using the personal data and there are no overriding legitimate grounds for the processing;

d. We are unlawfully using the data.

Where we are using the personal data lawfully in a manner which is necessary for us to perform a contract between us and the individual, the right to erasure will not apply.

17. Transparency

The first data protection principle requires us to be transparent in relation to the personal data which we use. This includes being transparent with the individuals whose personal data we process and also being transparent with the Information Commissioner's Office.

Privacy Notices
When collecting information from a Data Subject, NDH should always inform them why the information is required and the use to which it will be put through a privacy notice.

a. We will be transparent and provide accessible information to individuals about how we will use their personal data. This will be done through the provision of privacy notices.

b. The information which we are required to provide to individuals in a privacy notice are set out in Articles 13 and 14 of the GDPR and will include the following information:

i. Our identity and contact details;
ii. The contact details of our Data Protection Officer;
iii. Our purpose for processing the personal data;
iv. Our legal basis for processing the personal data;
v. Our legitimate interests for using the data (if this is the lawful basis on which we rely);
vi. Any third parties with whom we share the personal data;
vii. Whether we transfer the personal data outside of the European Economic Area, and details of the safeguards for such a transfer (including details of adequacy decision);
viii. the period for which the data will be stored;
ix. description of individual's rights;
x. the right to withdraw consent (if consent is the lawful basis on which we are relying);
xi. the right to lodge complaint with the Information Commissioner's Office;
xii. any statutory or contractual requirement which we are relying on to process their personal data;
xiii. where the personal data is required to enter into a contract;

c. We have created privacy notices for different categories of individuals which are:

i. The Employee Privacy Notice
ii. The Customer Privacy Notice
iii. Privacy notice for job applicants
iv. Website privacy policy (and cookies notice)

d. It may be necessary to have tailored notices where extra information is collected, processed and shared, e.g. if extra support is provided to vulnerable residents or where employment advice is provided, etc.

e. As appropriate the Privacy Notices are published on our website and/or intranet.

18. Data portability

The right to data portability enables individuals to acquire and reuse their personal data for their own purposes across different services. On request, the data must be provided to the Data Subject in an organised, frequently used and machine readable format and be provided for free and within one month.

Our current IT systems do not allow data to be extracted in this way so in the event of any request received, various options will be explored with the requestor as to an appropriate data format. In order to ensure future compliance with this Right, any new housing management system specification will include this requirement.

19. Accountability and Data Management

DATA PROTECTION BY DESIGN AND DEFAULT

a. The GDPR requires us to consider data protection by design and default. This obligation requires us to consider the data protection implications of any project or process both at the point of inception and throughout the life of any processing. Data protection is something which should also be a consideration in relation to everything and anything we do with personal data.

b. Those who use personal data on our behalf are required to consider data protection by design and default.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

c. A DPIA is an essential tool for demonstrating our compliance with the GDPR and the accountability principle. It is used to work out the impact which our use of personal data will have on individuals and is required by law if our use of personal data is likely to result in a high risk to individuals.

d. Where our use of personal data is likely to create a high risk to individuals, a DPIA should be completed before a new project or operation involving personal data begins. The DPIA should be completed in accordance with the DPIA procedure.

RECORD KEEPING

e. Under the GDPR, we are required to maintain records of our data processing activities. Those records shall be created, maintained and held by the DPO.

NDH's information asset register categorises data in terms of personal data and personal sensitive (special category) data. New types of data will not be acquired without approval by the DPO.

20. Sharing data with others

In order to share personal data with any third party we must have a lawful basis for doing so. Apart from in limited exceptional services, we will also need to inform the individual about such sharing in advance through the privacy notice.

In limited circumstances, we may disclose personal data to an organisation without first informing the individual beforehand. An example may be where the sharing of data is necessary for the prevention and detection of a crime. Under such circumstances, staff will ensure the request is legitimate, and seek guidance from the DPO.

Where we share personal data with a third party organisation, either regularly or for one off project, we shall consider whether a data sharing agreement and/or non-disclosure agreement is appropriate in the circumstances. If a data sharing agreement is completed, this will be recorded on the Information Asset Register. NDH may use its own standard data sharing agreement template or the third parties if we are satisfied that this is suitable and adequate for the purposes.

Children merit specific protection with regard to their personal data, ordinarily staff will be expected to seek the consent of the person with parental responsibility if a safeguarding referral is going to be made, if it is likely to place the child at

increased risk, the decision to not seek consent can be taken.

21. Contracts

All contracts will set out the requirements for compliance with the GDPR and the third party arrangements for ensuring any information shared is retained in line with GDPR. This is particularly relevant where another organisation is processing personal data on our behalf as the GDPR imposes strict requirements in relation to the need to have a written contract in such situations and also the clauses which must be included in such an agreement.

Compliance with GDPR will also be a standard requirement for any Data Sharing Agreement or Non-Disclosure Agreement. As far as possible, any data shared will be through an appropriately secure method, e.g. encrypted email or secure portal.

22. Transferring personal data to a country outside the European Economic Area

We will not transfer any personal data outside of the European Economic Area unless the DPO has confirmed that such a data transfer is lawful and appropriate in the circumstances.

In the event that data is approved to be transferred outside of the EEA, in line with Chapter 5 (Article 23) of the GDPR we will ensure that appropriate safeguards are in place for example Privacy Shield in the US or that data is transferred to another 'Adequate Country'.

23. Data risks, breaches and security

a. This policy helps to protect NDH from some very real data security risks including:

i. **Breaches of confidentiality –** information being shared or made public inappropriately.
ii. **Reputational Damage -** For instance, the company could suffer if sensitive data was accessed by hackers.
iii. **Loss of Customer Trust** – customers no longer provide information.
iv. **Minimising the risk of fines through compliance with this policy** (as impact of a fine is a significant risk, however likelihood is rare if robust policies and procedures are in place).

b. As part of our commitment to GDPR and risk management, NDH will maintain Cyber Essentials accreditation to help limit the cyber risk in relation to potential cyber-related GDPR breaches.

Reporting of data breaches

c. Anyone who is using personal data on our behalf is required to report <u>all</u> actual or potential data protection compliance failures (near misses) and breaches to the DPO or their line manger who will pass on the information to the DPO as soon as they are discovered.

This allows us to:

i. Investigate and take any required remedial actions if necessary.

ii. Maintain a register which can be monitored and record lessons learned.

iii. Report and formally note at the Information Compliance Security Group meeting. (via their line manager or head of service)

iv. Notify the ICO in line with the GDPR timescale of 72 hours.

d. The Security Breach Guidance contains further information on how to report a breach and action to be taken.

Data security for employees

i. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
ii. **Strong passwords** must be used, changed in line with set IT policies and they should never be shared.
iii. Personal data **will not be disclosed to unauthorised people**, either within the company or externally.
iv. Employees will make sure paper, printouts or files are **not left where unauthorised people can see them**, e.g. meeting rooms or on a printer.
v. As set out in the staff handbook, NDH operate a **clear desk** policy ensuring that any documentation (paper or files) should not be left out but kept in lockable drawers or cabinets.
vi. Ensure that **computer screens are locked** whenever they are left unattended.
vii. Data printouts should be placed into shred it bins provided and disposed of securely when they are no longer required.
viii. Employees will not save copies of personal data to their own home computers or NDH PC c: drives.
ix. Where possible personal data will not be sent by standard email, as this form of communication is not secure. Data should be encrypted before transferring electronically.

24. Monitoring and compliance

External assurance will take place in line with the Audit and Risk Committee's internal audit plan or specialist review at regular appropriate intervals but at least every 5 years.

25. Data retention and disposal

NDH will keep different types of information for longer than others. All employees are responsible for ensuring that information is not kept for longer than necessary in accordance with the NDH Data Retention Policy.

Where personal and confidential information is no longer required, it will be destroyed in a secure manner.

26. Accompanying policies and procedures

This Policy is the overarching document for NDH's Data Governance Framework. Other documents which form part of this framework are:

a. Data Security Breach Procedure
b. The Subject Access Request Procedure and Register
c. Data Protection Impact Assessments Procedure
d. The Information Asset Register
e. The Data Retention Policy
f. Clear Desk Policy (contained in staff handbook)
g. Cyber Security policy
h. Information Security policy
i. Privacy notices.

Written by:	**Appendix:**
Philippa Butler Finance Director (and DPO) 24 May 2018 Updated: 2 September 2019	None.
Next Review Date November 2021	1st September 2019