Data Protection & Privacy **Policy**

Issue Number: 06 **Reviewed: May 2018**

Responsibility: Business Transformation **Next Review Date: May 2020**

Introduction

This policy covers how Hightown complies with the EU General Data Protection Regulations (EU) 2016/679 (GDPR) for all the data it holds on living individuals (Tenants, Employees, Service Users etc.). This includes data held electronically, in hard copy, images and verbal.

People using our services have the right to expect that information given in confidence will be used for the purpose for which it was given and will not be released to others without their consent. The information provided should be accurate, relevant to the Association's work, kept no longer than necessary and properly protected.

More detail regarding GDPR can be found using the following links:
GDPR: https://ico.org.uk/for-organisations/data-protection-reform/

1. Data Protection Officer
   a) The Data Protection Officer referred to throughout this policy is a specific role within the organisation under GDPR. The nominated Data Protection Officer is the Director of Business Transformation.

2. General Handling of Data
   a) All staff handling personal and sensitive information about employees or people using our services will treat this information in a discreet and confidential manner and in a way that they themselves would wish their own information to be handled.

   b) All personal information will be treated as private and will only be accessible to relevant employees of the Association. Electronic documents must not be left open on computers and paper documents should not be left lying around on desks. No personal data will be stored on the hard drives of laptops or mobile devices.

   c) Written records and correspondence must be kept secure at all times and locked away when not in use.

   d) When disposing of personal and confidential information staff will use the confidential waste bins provided throughout the office. Under no circumstances should documents containing personal information be put in general waste bins. Staff based at C&SH sites will dispose of confidential waste through shredders where they are provided, or arrange disposal at the main office or through a bulk collection by a certified confidential waste disposal company.

   e) Only personal information relevant to the Association's business should be kept in documents or databases. Any other information should be deleted.

f) Staff should ensure that any changes to personal details are accurately and promptly recorded on the appropriate records and that suitable verification has been carried out.

g) All data protection guidance applies to personal information processed verbally in phone calls, meetings and conversations. The same standards of privacy and confidentiality apply and conversations and phone calls should not take place in situations where they may be overheard, e.g. corridors, shops, cafes.

h) All data protection guidance applies to information about work colleagues and personal information such as home address and personal mobile numbers should not be passed to a third party without consent.

3. Sharing Data with Third Parties

a) Information can be passed to other organisations and professionals but only if it is for assisting the Association to carry out its normal tasks and only in accordance with the relevant Privacy Notices. Otherwise it should not be shared without additional specific consent (see below).

b) Any request for personal data based on an exception (e.g. giving information to the Police or Tax authorities) should be checked with the **Data Protection Officer before any information is provided.**

c) Particular care should be taken with large lists of data (e.g. contact details sent out to contractors, or resident/service user information shared with other housing organisations, care agencies, benefit agencies). Secure email should be used, or files should be password protected and encrypted. The IT department can assist staff in providing this data in a secure manner.

4. Subject Access Requests

a) Individuals are entitled to make Subject Access Requests for all or part of the data held on them. Care must be taken to ensure the authenticity of people requesting information and written requests for data should be asked for and recorded.

b) Requests for data should be processed in a timely manner and take no longer than 1 calendar month. Hightown will provide the data free of charge unless the request is deemed unfounded, excessive, or repetitive.

c) In the case of excessively large or repetitive request for data, we may ask for the request to be more specific, extend the response time by 30 days and/or charge for the work. The decision to do this will be made by the **Data Protection Officer**.

d) Any breach of confidentiality will be regarded as misconduct and is subject to the Association's disciplinary procedure as well as potentially being a criminal offence.

e) Reports written by a third party requires their consent to distribute.

5. Data Breaches

a) Any breach of data protection, or a suspected breach, will be reported to the **Data Protection Officer** who will then be responsible for to informing the Information Commissioner within 72 hours if required, ensuring that as much as is reasonably possible is done to reduce the impact of the breach, and reviewing any systems in place that could be improved to reduce the likelihood of a breach happening again.

Examples include:

- Loss of an unencrypted electronic storage device
- Inappropriate access to personal data due to lack of internal controls
- Sending an email with personal data to the wrong recipient
- Deleting personal data without authorisation.

6. Retention

a) Documents will be retained in accordance with the latest Document Retention guidelines for Housing Associations published by the NHF and attached in Appendix1.

7. Privacy Notices and Explicit Consent

a) The majority of Hightown's activities are covered under Legitimate Interests with regard to consent within GDPR. Hightown has published Privacy Notices for customers and for staff that are accessible from the website and outline the personal data we collect, why we collect it and the rights of the individuals whose data is processed.

b) Where Hightown relies on Legitimate Interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees, residents or service users and has concluded that they are not.

c) Where special category data is processed, this is only done with the explicit consent of the individual and this is made clear when the data is collected. This consent may be withdrawn at any time and for any reason.

d) New service users, residents, and staff will be asked to confirm they have read and accepted the appropriate Privacy Notice prior to signing up. Information on how to access Privacy Notices will also be prominently displayed where data is collected.

8. Vital Interests

a) Personal data will be lawfully processed without consent in the rare circumstance where information is passed to a 3rd party in a situation where withholding the data would result in a clear threat to an individual's life and the individual is physically or legally unable to give consent themselves. For example informing paramedics that an unconscious person is a diabetic.

9. Direct Marketing

Hightown carries out limited direct marketing for sales and lettings, and to inform residents and service users about services we provide. Information is only sent to customers who have opted in to the service. Customers can opt out at any time by updating their preferences in the resident portal or by notifying Hightown in writing.

10. Automated Decision Making

11. Hightown has one automated decision-making process, this is where a driving licence and access to a vehicle are essential for specific posts. This decision-making is necessary to ensure the applicant has the capacity to enter into a contract of employment where car usage is essential, and to avoid the risk of infringement of relevant road safety legislation such as the Road Traffic Act 1998.

Data Mapping

a) The Association carries out data mapping exercises and they are kept up to date through annual review. The mapping process identifies the following:

i. What personal data is held?
ii. How is it collected?
iii. What is it used for?
iv. Where is it stored?
v. Who has access?
vi. How is it kept safe?
vii. Who is the data shared with?
viii. How long is it kept for?
ix. What is the Lawful Basis to Process it?

12. Right to Erasure (aka Right to be Forgotten)

a) Individuals have the right to be forgotten within our systems. The following paragraphs outline when and how this would be carried out.

b) Residents
   i. Any resident wishing us to consider an erasure request must be a former tenant for at least 7 years and have no outstanding debt or credit with us.
   ii. The client, tenancy and rent account records are not formed entirely of personal data. We will anonymize or delete the data in all fields relating to name, date of birth, NI number, bank details, and all addresses not relating to the Association's property. This method allows us to keep statistical and historical records, whereas deletion would not.

c) Employees
   i. Any employee wishing us to consider an erasure request must have ceased all employment with us, have no pension, and no outstanding debt or credit with us and have ceased working for us for 20 years.
   ii. We will anonymise the former employee's name, addresses, telephone numbers, email addresses, NI number, bank details, and next of kin details.

d) Service users
   i. Any service user wishing us to consider an erasure request must no longer be receiving support from us for at least 7 years, and have no outstanding debt or credit with us.
   ii. The service user, tenancy, and rent account records are not formed entirely of personal data. We will anonymize or delete the data in all fields relating to name, date of birth, NI number, bank details, and all addresses not relating to the Association's property. This method allows us to keep statistical and historical records, whereas deletion would not.
   iii. We will also destroy all records of care provided as allowed by law.

e) In all cases, the erasure request will be managed by the Head of IT and will require the approval of Data Protection Officer and another Director.

13. Responsibilities of Director of Business Transformation

a) To act as the **Data Protection Officer** for the Association ensuring it is registered with the Data Protection Registrar, and to manage correspondence with them.
b) To deal with reported breaches and notify the Information Commissioner within 72 hours where necessary.
c) To be the principal point of contact for advice on Data Protection issues.
d) To ensure that Privacy Notices for Support, Residents, and Staff are available and reviewed regularly.
e) To implement processes for dealing with requests for access, rectification, erasure, restricting processing, data portability and objections.
f) To ensure that the Data Mapping exercise is completed and review annually.
g) To ensure that training is available for staff with regard to GDPR.

14. Responsibilities of the Head of IT

a) To provide easy and secure access for staff to the Association's data on the network via desktop computers or remotely through the Citrix portal. (to avoid the need for staff to download information onto USB sticks or email it to themselves at home etc)
b) To manage and administer appropriate departmental and role specific access to the Association's databases and network folders.
c) To provide advice to staff on Data Protection Issues.
d) To support members of staff in collecting personal data for subject access requests.
e) To enable rectification, erasure, restricting processing, data portability where this is has been agreed.

15. Responsibility of the Communications Manager

a) To check that appropriate consent has been obtained for marketing and promotional activities, where consent is the appropriate lawful basis.
b) To manage and administer the association's Photo Library ensuring that consent has been obtained for all photographs where required.

16. Responsibilities of all Directors

a) To ensure they have adequate procedures in place to store paper documents and files securely and that electronic information including images is being saved and stored securely in accordance with the Association's policies and procedures.
b) To ensure that the Data Protection Officer is made aware of the setting up of additional systems containing personal information within the department or changes to existing arrangements for storing this data.
c) To ensure that Data Protection Impact Assessments are carried out as appropriate for all new and amended processes.
d) To ensure that their staff are aware of the responsibilities as outlined in this policy.
e) To identify data breaches and potential breaches and notify the Data Protection Officer
f) To identify staff training needs and ensure all staff receive data protection training appropriate to their role

17. Further guidance

Staff will read this policy in conjunction with the staff handbook and relevant procedures on Hightown's intranet.