HOUSING GATEWAY LIMITED

DATA PROTECTION POLICY

Adopted November 2020

CONTENTS

1. INTRODUCTION

1.1 Housing Gateway Limited (HGL) is required, as part of its overall information governance structure, to ensure that appropriate controls are implemented and maintained in relation to the collection, use and retention of personal information pertaining to its customers, clients and staff and that these are in accordance with the requirements of the Data Protection Act 2018 (the Act) and the UK General Data Protection Regulation created from the original EU GDPR by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, along with other regulations. We will refer to these as the "data protection law".

1.2 This document provides a framework for HGL to meet legal requirements in relation to requests that fall within the scope of the data protection law.

1.3 The Policy applies to all personal information created, received, stored, used and disposed of by HGL irrespective of where or how it is held.

1.4 It must be noted that the data protection law is a 'legal' requirement and that individuals can face prosecution for breaches of it and can be fined as individuals.

2. AIM OF POLICY

2.1 The aim of this document is to clarify HGL's legal obligations and requirements for the processing of personal data and to ensure that all such data is:

- collected, stored and processed for justifiable business reasons which were notified to the data subjects when collected
- used only by those persons with a legitimate reason
- stored safely
- retained only for the defined time period
- not disclosed to unauthorised persons.

2.2 HGL will actively seek to meet its obligations and duties in accordance with the data protection law and in so doing will not infringe the rights of its employees, customers, third parties or others.

3. SCOPE

3.1 The scope of this policy requires compliance with the Data Protection Principles which are defined in the data protection law.

Personal Data is defined as: personal data relating to an identifiable living individual and includes the expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. The individuals about whom we hold personal data are called "**data subjects**"

Special Category personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- physical or mental health or condition
- sexual life or sexual orientation
- commission of criminal offences or alleged offences.
- Generic data
- Biometric data for the purposes of uniquely identifying an individual

3.2 Extra protection needs to be given to special category personal information and it may require additional security measures to ensure both its integrity and security. Special category data also requires additional legal justification for use.

4. DATA PROTECTION PRINCIPLES

4.1 The data protection law is underpinned by a set of six common-sense principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

4.2 All personnel processing personal information during their business functionality must ensure they adhere to the Data Protection Principles which require that personal data shall:

- Be processed lawfully, fairly and in a transparent manner in relation to the data subject

- Be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (there are also further rules on archival use)

- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- Be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

- Not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (again, there are additional rules about archival use)

- Be 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

5 THE INFORMATION COMMISSIONER'S OFFICE

5.1 The Information Commissioner administers the data protection law in the UK. The role and duties of the Commissioner include:

- ensuring compliance with the data protection law

- ensuring that individuals rights to privacy are respected

- ensuring that individuals have access to data held about themselves

- establishing and maintaining a Register of Fee Payers and making it publicly available

- investigating complaints, serving notices on data users who are contravening the principles of the data protection law, and where appropriate prosecute offenders.

5.2 The data protection law gives the Information Commissioner wide powers to ensure compliance with the data protection law, including warrants to search and seize documents and equipment.

6 ACCESS AND USE OF PERSONAL DATA

6.1 This policy applies to everyone that has access to personal data and includes any third party or individual who conducts work on behalf of HGL or who has access to personal data for which HGL is responsible and who will be required contractually or otherwise to comply with this policy.

6.2 Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

6.3 It is an offence for any person to knowingly or recklessly obtain, procure or disclose personal data, whether for gain or not, without the permission of the data controller (HGL) subject to certain exceptions.

6.5 All personnel (staff or customers) are entitled to:

- Know what information HGL holds and processes about them and why it is held
- Know who can gain access to it
- How to keep this data up-to-date
- Know what action HGL takes to comply with its obligations under the data protection law.

6.6 HGL will ensure that compliance with this Policy is monitored and is able to evidence that it is complying with its legal responsibilities with respect to its staff and customers.

7 HOUSING GATEWAY'S COMMITMENT

7.1 To achieve the overall aim of the Data Protection Policy, HGL will:

- Provide adequate resources to support an effective corporate approach to Data Protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise HGL's commitment to Data Protection.
- Compile and maintain appropriate procedures and codes of practice.
- Promote general awareness and provide specific training, advice and guidance to its staff at all levels and to its Members to ensure standards are met.
- Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

8 ROLES AND RESPONSIBILITIES

8.1 Ultimate accountability for all decisions made relating to the data protection law lies with the **Board of Directors**.

8.2 The **Board of Directors** is responsible for ensuring that sufficient resources are provided to support the requirements of this policy as well as making strategic level decisions which impact on how HGL carries out

its obligations under the legislation. Each Director is responsible for monitoring compliance and taking any necessary corrective action.

8.3 **Information/System Owners** have a responsibility to ensure that data stored on systems is captured, stored, processed, accessed and deleted in line with the data protection law.

8.4 **All HGL employees** and personnel working with personal data have a responsibility to ensure that they have sufficient awareness of the data protection law so that they can comply with the requirements of the law.

9 RESPONSIBILITIES OF STAFF, DIRECTORS & THIRD PARTY CONTRACTORS

9.1 The processing of personal data is to be compliant with legal, industry, regulatory and business requirements; it is the responsibility of staff, Directors and third-party organisations providing services on behalf of HGL to be aware of and conversant with these requirements for the processing and management of personal data in an appropriate manner.

9.2 Staff, Directors and third-party organisations providing services on behalf of HGL will need to be aware of how staff, Directors and third party organisations providing services on behalf of HGL safeguards its data and ensure that the appropriate protective marking is applied to all information. In most cases personal information about any living individual will attract the classification of OFFICIAL-SENSITIVE [PERSONAL].

9.3 The following minimum requirements are applied to everyone who encounters personal data:

- Ensure that personal data is to be processed accurately and only for a specific purpose. If data needs to be used for a different purpose then the consent process will need to be repeated

- When not required for immediate use personal data is to be secured from unauthorised viewing and access

- Personal, sensitive and restricted data must not be sent to/from personal/staff/member home email accounts

- Personal information can only be distributed externally through email if it is:
  - password protected and encrypted or
  - via secure email (e.g Secure Office 365 mail) or
  - via a Secure Enhanced File Transfer facility.

- Computer systems that process, access or store such data are to have password protected screen savers activated when left unattended.

- The carrying of personal, sensitive or confidential information outside secure office environments should be avoided wherever possible. If this is unavoidable, then staff, Directors and third-party organisations providing services on behalf of HGL should use encrypted laptops where possible. Documents holding personal or sensitive information should be carried separately to the laptop case.

- When no longer required to be retained all personal data is to be disposed of securely, i.e. by shredding or via secure waste disposal.

- Personal data may not be stored on removable media devices without explicit management approval and appropriate encryption controls. Such data is to be removed from the removable media as soon as practically possible.

- The discussion of personal data with unauthorised persons either inside or outside HGL is expressly prohibited. This also includes, but is not limited to, email, social networking sites, blogs, forums, instant messaging services, chat rooms etc.

- Any staff directly employed by HGL will be required to undertake Data Privacy and Information Security training on joining the organisation and as required thereafter.

10 DATA CONTROLLER

10.1 In accordance with the data protection law, HGL as a corporate body is the Data Controller and is therefore ultimately responsible for the implementation of this policy.

10.2 HGL staff responsible for the day-to-day management of the data within their business areas of responsibility are required to ensure that the data protection law is complied with, including but not limited to:

- all data is processed fairly, including publication of notices as required by the data protection law

- the data is accurate, and that processes exist to check, amend and delete data as necessary

- consent, where required, is obtained and recorded, and that a data subject is not misled/deceived as to why their data has been collected

- policies and procedures are in place to enable access by those who the data concerns and data subjects should be advised who is holding and using their data

- data is held securely

- data is disposed of properly

- notification requirements are satisfied

- determination regarding processing of data without consent are made, especially in cases of public interest.

11 DATA PROTECTION OFFICER (DPO)

11.1 The DPO is responsible for HGL's registration with the Information Commissioners' Office (ICO), and for ensuring HGL complies with current legislation.

11.2 The DPO will monitor that appropriate 'fair processing' statements are made when HGL, its agents, contractors or service providers collect or process personal information for which HGL is the Data Controller, reflecting the purposes for which the information may be used and any other parties to whom the information may be revealed.

11.3 The DPO will conduct periodic reviews of computer and hard copy records to verify that HGL is acting in accordance with the data protection law.

11.4 The DPO will respond to complaints about how we have processed personal information relating to individuals; this must be within 21 days of receipt. The response must explain the actions (if any) HGL will take.

11.5 The DPO will keep Directors and any directly employed staff informed of data protection issues pertaining to HGL, including any changes in legislation that might impact business processes.

11.6 The DPO will ensure that Data Privacy and Information Security training is available to staff and that a record of completion is maintained.

11.7 The DPO must be consulted on any proposed new or changed uses of personal information before any change in process or additional information collection is authorised. If HGL decides not to follow the DPO's advice, this must be formally recorded and communicated back to the DPO.

11.8 If a member of staff or customer (or an authorised person acting on their behalf) submits a request to exercise their rights under the data protection law regarding the personal information held about them the DPO must ensure that relevant staff are aware of the processes required and the appropriate timescales for response.

12. TRAINING AND AWARENESS

12.1 All HGL employees have a responsibility to ensure that they and the staff they manage have undertaken Data Privacy and Information Security

training and have sufficient awareness of the data protection law so that they are able to comply with the requirements.

12.2 It is mandatory that all HGL staff (including temporary or casual workers) that have access to personal data or to the corporate network to undertake the Data Privacy and Information Security training. New entrants will be expected to undertake and successfully complete the module as part of the corporate induction process. Established staff will be expected to undertake and complete refresher training as directed.

12.3 Managers should encourage and make time for their staff to attend any further Data Privacy and Information Security training or awareness opportunities that may arise.

12.4 Failure to complete the courses within the prescribed period could result in disciplinary action proceedings.

13. COLLECTION OF DATA

13.1 HGL collects and records personal data from various sources, including that obtained or provided by the data subjects themselves.

13.2 In some instances data may be collected indirectly through monitoring devices, including but not limited to: door access control systems, CCTV and physical security logs, electronic monitoring systems.

14. ACCURACY AND RELEVANCE

14.1 It is the responsibility of those who receive personal information to ensure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to ensure that it is still accurate.

14.2 If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected.

15. RIGHTS TO ACCESS INFORMATION

15.1 All data subjects have the right to access any personal information (data) about them that is held or processed on computer or in certain hard copy files. Before access to this data is authorised a Subject Access Request form is to be completed and handed to an approved officer for processing.

15.2 HGL aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 1 month unless there is a good reason for any delay. In such cases the reason for a delay will be explained in writing to the person making the request.

16. FAIR AND LAWFUL PROCESSING

16.1 When HGL processes personal data, it must have a lawful basis for doing so. Data protection law provides a list of conditions to ensure that personal information is processed fairly and lawfully:

- Personal information is only processed where it is justified, in accordance with Article 6 of the UK General Data Protection Regulation.

- That sensitive personal information is processed only where necessary and justified, that such processing is undertaken only by the appropriate persons in accordance with Article 9 of the UK General Data Protection Regulation.

16.2 Individuals that supply HGL with personal information are provided with a 'Privacy Notice' (or online privacy statement) which communicates the information required by Article 13 and, where necessary, Article 14 of the UK General Data Protection Regulation.

17. DATA SHARING

17.1 Where HGL shares personal information with any third party a 'Data Sharing Agreement' is to exist as part of a formally documented written agreement or contract.

17.2 Where the other party uses the personal information for its own purposes:

- The agreement or contract will clearly describe the purposes for which the information may be used and any limitations or restrictions on the use of that information

- The other party is to provide an undertaking or provide other evidence of its commitment to process the information in a manner that will not contravene the Data Protection Law.

17.3 Where the processing of personal information with a third party is required by law, procedures are to ensure that the protocols and controls for the sharing of the data are documented, regularly reviewed and verified.

17.4 Requests for personal information from the Police or other enforcement agencies may be made in accordance with Schedule 2 of the Data Protection Act 2018. These must be individually reviewed to confirm if HGL is able or required to comply.

18. DATA RETENTION AND DISPOSAL

18.1 HGL is to ensure that personal information is not kept for any longer than is necessary; this is to adhere to any legal, regulatory or specific business justification.

18.2 HGL will retain some forms of information longer than others, but all decisions are to be based upon what is permissible under data protection law and will be published as HGL's retention schedule.

18.3 When disposing of information, equipment or media, this should be done confidentially.

19. TRANSFER OUTSIDE OF THE UK & EEA

19.1 To ensure an adequate level of protection is applied to personal information transferred or processed outside the UK & European Economic Area (EEA) contracts are to include conditions relating to the specific requirements for the protection of the information.

19.2 HGL is responsible for ensuring that 'due diligence' is conducted on the other party, and that adequate and appropriate controls and safeguards are applied for the transfer of the personal information.

19.3 Companies outside the UK & EEA are to be required to apply the same controls and requirements as applied within the UK & EEA unless they can demonstrate other adequate procedures are implemented to protect the personal information as part of the 'due diligence' process. Periodic reviews of the same are to be conducted to ensure adherence is maintained.

19.4 Under the data protection law, HGL is responsible as data controller for ensuring that data processors it instructs abide by these rules.

20. VIOLATIONS & BREACHES

20.1 Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct and could lead to termination of employment.

20.2 In the case of third parties unauthorised disclosure could lead to termination of the contractual relationship and in certain circumstances this could give rise to legal proceedings.

20.3 A data breach can occur for a variety of reasons (this list is not exhaustive):

i. Equipment failure
ii. Loss or theft of equipment, including mobile and portable devices
iii. Loss of paper records

iv. Human error
v. ‘Blagging’ offences where information is obtained by deceit.
vi. Inappropriate access controls
vii. Hacking
viii. Environmental disasters such as floods or fire

20.4 HGL requires all data security breaches by staff, agents, contractors or service providers to be reported to HGL or the DPO. The DPO will:

i. Assess the ongoing risks associated with the data security violation, implement and will implement an appropriate course of action.
ii. Determine an appropriate course of action for containment and recovery
iii. Determine who needs to be notified
iv. Investigate the cause of the breach