Data Protection - Group Policy

Policy owner/author:	Policy & Performance Coordinator
Team:	All
Date approved:	18 May 2023
Approved by:	Audit & Risk Committee/ Board of Management
Review Dates	July 2020 March 2015

1. Policy Statement

Honeycomb Group (HG) holds personal and confidential information about individuals. We recognise that all individuals have a right to data privacy. We will comply with the terms of the Data Protection Act (DPA).

Our policy aims to protect the rights of individuals and HG. It identifies information that is to be treated as confidential and the procedures for collecting, storing, handling, and disclosing such information.

Our policy covers all records and information held by HG and the confidentiality of information held about individuals.

We have appointed a designated person within the organisation (HG's Data Protection Coordinator) who takes a lead role for responding to data protection enquiries and ensuring systems for data capture, storage and disposal are fit for purpose.

We will respond to all requests for data protection information promptly and courteously. We will acknowledge all written requests for data protection information within three working days and, subject to verification of an individual's identity being confirmed, will provide a full response within 30 calendar days, including requests for individuals' own images captured on HG owned CCTV systems.

We will provide all new staff with data protection and information security training as part of their induction process and all other staff will receive refresher training as

required. All staff will be required to read the Data Protection Policy and ICT System and Data Security Policy.

Where personal data is to be sent electronically, staff will ensure that the data is encrypted using approved procedures.

All staff and customers will be offered a private place to discuss anything of a personal or confidential nature when requested.

We will adhere to the latest guidance and codes of practice produced by the ICO.

We will comply with any recommendations or judgements made by the ICO if it is found to have broken the Data Protection Act.

2. Definitions

Data processing - any activity performed on the personal data. It includes any use, disclosure, storage, or collection of personal data.

Data Protection Act (DPA) 2018 – sets out how personal information is used by organisations, which must ensure information is used fairly, lawfully and for limited, specifically stated purposes.

Data subject – is the individual about whom the personal data relates**.** This includes employees, board members, employment applicants, volunteers, tenants, housing applicants, all service users, and suppliers.

General Data Protection Regulation (GDPR) - legislation enforceable from May 2018 gives strict rules on the collection, processing, storage, and use of individuals' personal data by organisations.

Personal data - means data relating to a living individual who can be identified from that data (or from that data and other information held). It can be factual (such as a name or a date of birth) or it can be an opinion (such as a staff performance review or service user support plan).

Sensitive Personal Data – a DPA concept which includes information concerning and individual's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual orientation, and criminal offences.

Special Categories of personal data is information that the GDPR says is more sensitive and relates to:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health condition
- Sexual life or sexual orientation

It is the type of data which could create more significant risks to a person's rights, for example by putting them at risk of unlawful discrimination. Processing this data is prohibited unless there is a lawful basis as set out in section 3 of this policy.

3. Data Protection – legal requirements

There are six data protection principles which HG will adhere to and help ensure compliance with the data protection legislation.

The six principles require that personal data (electronic and paper records) should be:

1. Fairly and lawfully processed
2. Collected and processed for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and up to date
5. Not kept longer than necessary and processed in accordance with the data subject's rights
6. Kept secure

The lawful bases for processing data are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. In the case of sensitive data consent must be explicit.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

The current Data Protection legislation is supported by other legislation. This includes:

- The Human Rights Act 1998, article 8:

'Right to respect for private and family life, home, and correspondence. There shall be no interference by a public authority with the exercise of this right (except where necessary for legal, security, safety reasons etc.)'

Although Registered Providers are not public authorities it is good practice to operate within the law applied to public authorities.

- Crime and Disorder Act 1998. This contains a requirement to release information relating to applications for orders such as antisocial behaviour orders and sex offenders' registers. Greater local partnership working, and information sharing is encouraged through this Act.

We will comply with all relevant legislation, guidance and good practice.

4. Responsibilities

Our Data Protection Policy applies to all staff, board members and volunteers. There is a collective responsibility to ensure we stick to the principles of data protection. Staff and board members are expected to act in line with our Code of Conduct.

The Commercial Finance Director is responsible for ensuring this policy and the supporting procedures are effectively implemented and that staff and board members comply with the policy.

All staff have a responsibility to inform their line manager and HG's Data Protection Coordinator if they become aware of any breaches of data protection and near misses. Any staff member who knowingly breaches data protection which leads to personal detriment may be subject to investigation in accordance with our disciplinary procedures.

The Data Protection Coordinator will keep a record of all breaches and near misses.

5. General policy

5a. Data Protection Usage

We will only collect, store and use personal data for legitimate business purposes and will not forward on information to any third parties. Where a law enforcement agency seeks personal data to assist in identifying an alleged offender, the `crime exemption' may apply.

Any special categories of personal data held will be used to tailor services to meet individuals' needs, for statistical purposes and to ensure the organisation fulfils its aims outlined in our Equality & Diversity Policy.

5b. Data Accuracy

We will minimise the opportunities for creating inaccurate data and we will make sure that data is corrected, modified, and updated as and when necessary.

Inaccurate data that is no longer needed will be securely erased. It is the responsibility of all staff to check the data they are using and to respond to reports of data inaccuracy from customers and colleagues.

5c. Data Storage

We will maintain high standards of data security at all times and in line with GDPR principles will ensure:

- All staff are aware of and abide by the ICT System and Data Safeguarding Policy
- There are appropriate measures in place to protect personal data including password protected computer systems and handheld devices, confidential waste arrangements, secure office accommodation and good practice guidance available to staff on sharing personal data.
- Sensitive personal data such as police restricted information or adult/children social care or safeguarding data is held outside of standard access customer records and access is restricted to authorised staff only.
- Contracts exist with any third party data processor who processes information on our behalf.

5d. Data Retention

We will not keep data for longer than it is necessary.

The Data Protection Act does not specific data retention periods as it recognises that the needs of Organisations will vary. We will use good practice guidance from relevant professional bodies to identify how long we should retain data.

Key guidance will include but is not limited to:
'*Document Retention Guide for Registered Social Landlords'* National Housing Federation - https://www.housing.org.uk/resources/document-retention-and-disposal-for-housing-associations/
Finance Conduct Authority - https://www.fca.org.uk/publication/systems-information/retention-schedule.pdf
HMRC – https://www.gov.uk/government/publications/hmrc-records-management-and-retention-and-disposal-policy/records-management-and-retention-and-disposal-policy
CIPD - https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet#gref

5e. Data Disposal

We will only hold and store personal information about individuals for as long as required within the provisions of the current data protection legislation.

When disposing of personal data, we will use registered confidential waste carriers who can provide certificates of destruction.

We will comply with current best practice and guidance when disposing of computer equipment and will ensure computer hard drives are cleansed to prevent any loss of personal data.

5f. Individuals' Rights

We acknowledge individual's rights in connection with personal data. The key rights are:

- **Right to be informed**

All staff, customers and other individuals are entitled to:

- know what information we hold and process about them and why;
- know how to gain access to it;
- know how to keep it up to date; and
- know what HG is doing to comply with its obligations under data protection legislation.

- **Right of subject access**

When a customer requests (in writing or electronically) a copy of their personal data, the purposes for which it is being processed and to whom it may be disclosed; a subject access request will be processed within thirty days.

- **Rectification, blocking, erasure and destruction**

A data subject may apply to rectify, block, erase or destroy their data if they think it is inaccurate or contains an opinion which is based on the inaccurate data. There is also a qualified right to erasure, known as the '**right to be forgotten'.** Data subjects can demand we delete or destroy their data on various grounds, including where retaining the data is no longer necessary.

- **A right to restriction**

In some cases, a data subject can demand that the further processing (other than storage) of their data is suspended**.**

- **A right to data portability**

Gives data subjects the right to receive their personal data from a controller in a 'machine-readable format' (such as a CSV file) and to have the data transmitted to another controller, where technically feasible.

Other rights include**:**

- **Right to prevent processing for purposes of direct marketing**
- **Right in relation to automated decision taking**
- **Right to compensation**

Exemptions

We will not normally share or pass on personal data to any third parties without the specific consent of the data subject.

There are certain situations where we do not have to obtain prior permission to disclose personal information about individuals. These include:

- To comply with the law (e.g. the police, Inland Revenue, Council Tax Registration Office or a court order) including the prevention or detection of crime or the assessment of tax.

- Where there is a health and safety risk (this will include information about customers with a history of violence and when other care professionals are involved in a customer's care).

- When there is evidence of fraud.

- In connection with legal proceedings or statutory action (e.g.to enforce compliance with tenancy conditions such as an application for possession or payment of Housing Benefit direct).

- The name of a customer and the date of occupancy to utility companies (where the customer is responsible for payment), providing the customer has been advised of this at the start of the tenancy or has given consent subsequently.

- Anonymously for bona fide statistical reporting or research purposes, providing it is not possible to identify the individual to whom the information relates (e.g. CORE returns).

- Where there are declarations of interest by staff, Committee or Board members.

- Where any staff may have concerns about a customer under the Safeguarding of Adults from Abuse policy or the Safeguarding Children policy.

- Where specifically enabled by the terms of registration of the GDPR

- The sharing is for the purpose of obtaining legal advice

- The individuals have given their consent

In addition to the above, there may be other circumstances where we will share information with third parties when the public interest in sharing the information outweighs the public interest in protecting confidentiality.

5g. Disclosure of Information

We will comply with the guidance in the Public Interest Disclosure Act which sets out the circumstances in which we are required or are able to share information without the explicit permission of the individual.

Personal information held will only be passed to another organisation on a need to know basis and with an individual's consent unless there are exceptional circumstances. Exceptional circumstances include:

- Where there is clear and evident fraud
- To comply with the law
- In connection with legal proceedings
- Where it would be essential to enable us to carry out our duties, e.g. where we believe that the health and safety of an individual would be at risk by not disclosing the information; or, where there is a legal requirement to do so. For example:
  - Where safeguarding concerns exist;
  - Where a person's 'vital interests' is concerned i.e. where sharing information is critical to prevent harm, distress or is required for medical intervention measures.

5h. Data Sharing Protocols

We will ensure data sharing protocols that exist with the Police and Local Authorities in the areas we operate adhere to guidance produced by the Association of Chief Police Officers and Association of Directors of Social Services.

This will include personal information relating to individuals that is shared in public protection forums such as:

- Safeguarding Boards (adults and children)
- Multi-agency risk assessment conferences (MARACs)
- Multi-agency public protection arrangements (MAPPAs)

We will ensure that where it is necessary for partners or contractors to share personal data about our customers, they will not pass this information on to any third parties without our consent. We will require that they agree to use the information only for the purposes it was originally intended.

5i. Use of CCTV Images

All CCTV images we capture are subject to the data protection legislation. In line with national guidelines CCTV images will be stored for as long as necessary to meet the purpose of recording them (up to 30 days).

Our Data Protection Coordinator will be the designated person for dealing with all data protection requests, including requests for the release of images captured by our CCTV Systems. (Further information is provided in our CCTV Systems procedure).

5j. Use of Photographs

Photographs of staff, customers, board members and the public will not be used without permission. Photographs of customers and the public will not be published in any form without signed permission.

No photographs of children will be published without the explicit signed permission of a parent/ guardian, and the permission of the child where this is appropriate.

5k. Internet and email

Although we permit our staff to use the email and internet for personal use (Internet and Email Acceptable Use guide), HG reserves the right to monitor such use to ensure that it is in accordance with this policy

Staff will be encouraged not to retain emails containing personal data for a period of longer than 28 days. After this date, if the data needs to be retained, it should either be electronically archived in a company database or be printed and stored in hard data copy in confidential files.

5l. Information Held

Individuals will be made aware of the reasons why personal information is required and held on record and the people likely to have access to it. Consent to disclose such information will be obtained from each individual and they will be informed of the implications of giving consent.

External contractors using HG systems will be expected to ensure they comply with our Data Protection Policy. Their access to our systems will be restricted to the areas they need, and Non-Disclosure Agreements will be agreed.

We will ensure any external systems used to store external data comply with the current Data Protection legislation. All information that is held will be relevant for the purpose for which it is required and stored securely.

5m. Childrens data

We work with children across our services, we recognise that children have the same rights as adults over their personal data. We also recognise that children may be less aware of the risks and consequences in relation to the processing of personal data.

We will ensure that children are addressed in plain clear, **age appropriate**, language **so they can understand how and why we hold, and sometimes need to share, their personal data.**

Transparency and accountability are important where children's data is concerned, and we recognise that is especially relevant when they are accessing our online services. We will ensure that children are aware of the risks of using online services and we will ensure our systems always follow best practice for safe use for children.

NB: when dealing with Child Protection information we don't necessarily need to get consent from the adults and/or children concerned to process data When we refer to a child we mean anyone under the age of 18. (Office of the High Commissioner for Human Rights, 1989)

See also our Child Protection Policy and procedure.

6. Complaints in respect of this policy

For staff, any complaints of breaches of confidentiality should be reported using our grievance procedure.

For all other individuals (such as job applicants, tenants, Glow, Concrete or Revival customers) any complaints of breaches of confidentiality should be reported to the Data Protection Coordinator using our complaints policy.

7. Training

All staff responsible for handling personal information will receive training on our Data Protection and ICT System and Data Security policy and it will be included as part of the new starter induction programme.

8. Linked Documents

This policy should be used alongside:

- ICT System and Data Security policy and procedures
- Data Protection procedures and guides
- Safeguarding policies and procedures