GH Property Management

The Right Choice.

Procedure for GDPR

1. Purpose

1.1 The purpose of this document is not to constitute legal advice. This procedure has been tailored to reflect GH's specific requirements following a data audit in accordance with the legislation, guidance and Codes of Practice issued by the Information Commissioner's Office.

2. Scope

2.1 This procedure applies to all Data controllers, Data Processors and Sub-Data Processors who are linked to GH Property Management Services Limited or have access to data held by GH Property Management Services Limited.

2.2 This procedure applies to current and former employees, Directors, workers, apprentices, Leaseholders and Residents. All individuals who fall into one of these categories, is a 'data subject' for the purposes of this document. This document should be read alongside a contract of employment or contract for services and any other notice we issue from time to time in relation to data held.

3. Procedure Statement

GH Property Management Services Limited takes the security and privacy of Employee and Client data seriously. We need to gather and use information or 'data' about Employees, Leaseholders and Residents as part of our business and to manage our relationship effectively with Staff and Clients. We comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify Clients of the information contained in this document.

GHPMS have separate privacy notices in place in respect of job applicants, Leaseholders, Residents, suppliers and any other relevant categories of data subject. A copy of these can be obtained from our website or upon request.

GHPMS has measures in place to protect the security of any data held.

GHPMS will only hold data for as long as necessary for the purposes in which we collected it.

The Company is a 'data controller' for the purposes of all personal data held on file. This means that we determine the purpose and means of the processing of any personal data.

This document explains how GHPMS will hold and process any information. It explains the rights of a data subject. It explains staff obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, GHPMS.

This procedure does not form part of any contract of employment or contract for services and can be amended by GHPMS at any time. It is intended that this document is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this procedure, GHPMS intends to comply with the 2018 Act and the GDPR.

4. Procedure

4.1 How will we process personal data?

GHPMS will process personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use personal data for:

- Performing the contract of employment or services
- Complying with any legal obligation
- If it is necessary for our legitimate interests or for the legitimate interests of someone else. Clients have the right to challenge our legitimate interests and request that we stop this processing.

We can process personal data for these purposes without knowledge or consent. We will not use personal data for an unrelated purpose without telling a data subject about it and informing them of the legal basis that we intend to rely on for processing it.

If a data subject chooses not to provide us with certain personal data, they should be aware that we may not be able to carry out certain parts of the contract between us. For example, if they do not provide us with bank account details we may not be able to pay them. It might also stop us from complying with certain legal

obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability.

4.2 When might we process personal data?

We need to process personal data in various situations during recruitment, employment or engagement with Clients and even following termination of employment or engagement with Clients.
For example:

- To decide whether to employ
- To decide how much to pay, and the other terms of a contract with us
- To check a data subject has the legal right to work for us
- To carry out the contract between us including where relevant, its termination
- Training staff and reviewing their performance
- To decide whether to promote employees
- To decide whether and how to manage staff performance, absence or conduct
- To carry out a disciplinary or grievance investigation or procedure in relation to an employee
- To determine whether we need to make adjustments to a workplace or role because of a disability
- To monitor diversity and equal opportunities
- To monitor and protect security, including network security of the Company, staff, Clients and others
- To monitor and protect the health and safety of all staff, Clients and third parties
- To pay employees and provide pension and other benefits in accordance with the contract between us
- Paying tax and national insurance
- To provide a reference upon request for another employer
- To pay trade union subscriptions where appropriate
- Monitoring compliance
- To comply with relevant laws such as, employment, immigration, health & safety, tax
- To answer questions from insurers in respect of any policies which relate to employees / Clients
- Running our business and planning for the future
- The prevention and detection of fraud or other criminal offences
- To defend the Company in respect of any investigation or litigation
- To comply with any court or tribunal orders for disclosure
- To ensure the smooth running of each block / development
- To maintain up to date block records
- To inform Clients of relevant updates or services

We will notify any data subject in advance of any other reason which may arise from time to time for processing personal data.
We will only process special categories of personal data in certain situations in accordance with the law. For example, we can do so if we have the data subject's explicit consent. If we ever ask for consent to process a special category of personal data, then we would explain the reasons for our request. A data subject does not need to consent and can withdraw consent later if they choose to by contacting the Data Controller.
We do not need consent to process special categories of personal data when we are processing it for the following purposes, which we may do:

- Where it is necessary for carrying out rights and obligations under employment law
- Where it is necessary to protect vital interests or those of another person where a data subject is physically or legally incapable of giving consent
- Where data has been made public
- Where processing is necessary for the establishment, exercise or defence of legal claims
- Where processing is necessary for the purposes of occupational medicine or for the assessment of working capacity

4.3 When might we share personal data?

Sometimes we might share personal data with contractors or other agents to carry out our obligations under our contract or for our legitimate interests.
Any company whom which we share personal data, we expect to keep personal data confidential and secure and to protect it in accordance with the law and our procedures. They are only permitted to process data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send personal data outside the European Economic Area. If this changes, data subjects will be notified of this and the protections which are in place to protect the security of data will be explained

4.4 How do employees process personal data on behalf of GH Property Management?

Everyone who works for, or on behalf of the Company has responsibility for ensuring data is collected, stored and handled appropriately.
The Company's Data Protection Officer is responsible for reviewing this document and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this document should be directed to the DPO.
Employees should only access personal data covered by this procedure if they need it for the work they do, or on behalf of the Company and only if they are authorised to do so. They should only use the data for the specified lawful purpose for which it was obtained.
Personal data should not be shared informally.
Personal data should be kept securely and not shared with unauthorised people.
Employees should regularly review and update personal data which they have to deal with for work.
Copies of personal data should be kept securely.
Unnecessary copies of personal data should not be made.
Staff should use strong passwords.
All computer screens should be locked when staff are not at their desks.
Personal data should be encrypted before being transferred electronically to authorised external contacts.
Personal data should not be saved to personal computers or other devices.
Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.
Any drawers and filing cabinets containing personal data should be locked.
No paper containing personal data should be left lying about.
Staff should not take personal data away from GH premises without authorisation from a line manager or Data Protection Officer and this should be done in line with our procedure for taking personal data outside of the GH office.
Personal data should be shredded and disposed of securely when it is finished with.
Staff should ask for help from our Data Protection Officer / Compliance Coordinator if they are unsure about data protection or if they notice any areas of data protection or security we can improve upon.
Any deliberate or negligent breach of this procedure by staff may result in disciplinary action being taken against them in accordance with our disciplinary procedure.
It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.

4.5 How do we deal with a data breach?

See procedure for dealing with data breaches, our data breach response plan & incident report log.
We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.
If anyone becomes aware of a data breach then they must contact The Data Protection Officer immediately and keep any evidence they have in relation to the breach.

4.6 What do we do when someone makes a subject access request?

See GH procedure for dealing with SARs.
Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. If a staff member receives such a request, it should be forwarded immediately to the Data Protection Officer/Compliance Coordinator who will coordinate a response.
GH must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.
There is no fee for making a SAR. However, if a request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to a request.

4.7 What rights do data subjects have?

A data subject has the right to information about what personal data we process, how and on what basis as set out in this procedure.

Data subjects have the right to access their own personal data by way of a subject access request (see above).

Any inaccuracies in personal data should be rectified.

A data subject has the right to request that we erase personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so they should contact the Data Controller / Compliance Coordinator.

Whilst requesting that personal data is corrected or erased or if contesting the lawfulness of our processing, a data subject can apply for its use to be restricted while the application is made. To do so they should contact the Data Controller / Compliance Coordinator.

A data subject has the right to object to data processing where we are relying on a legitimate interest to do so and they think that rights and interests outweigh our own and they wish us to stop.

The right to object if we process personal data for the purposes of direct marketing.

The right to receive a copy of personal data and to transfer personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, data subjects have the right not to be subjected to automated decision-making.

Data subjects have the right to be notified of a data security breach concerning their personal data.

In most situations we will not rely on consent as a lawful ground to process personal data. If we do however request consent to the processing of personal data for a specific purpose, data subjects have the right not to consent or to withdraw consent later. To withdraw consent, a data subject should contact the Data Controller / Compliance Coordinator.

A data subject has the right to complain to the Information Commissioner. This can be done by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on rights and our obligations.

5. Responsibilities

5.1 The CEO is the named Data Protection Officer (DPO) and is responsible for overseeing the GH data protection strategy and implementation to ensure compliance with GDPR requirements.

5.2 The Compliance Coordinator works alongside the DPO to oversee the GH data protection strategy and implementation to ensure compliance with GDPR requirements

5.3 All GH staff are data processors and are responsible for assisting the DPO in compliance with GDPR requirements.

5.4 Sub-processors, such as contractors, accountants and IT support agencies are responsible for following GH procedures to ensure compliance with GDPR requirements.

6. Definitions

6.1 '*Personal data*' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This document applies to all personal data whether it is stored electronically, on paper or on other materials.

Types of personal data we may collect and store:

- Recruitment information such as application form and CV
- References
- Qualifications and membership of any professional bodies
- Details of any pre-employment assessments
- Contact details and date of birth
- Contact details for emergency contacts
- Gender
- Marital status and family details
- Information about contract of employment or services including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement

- Bank details and information in relation to tax status including national insurance number
- Identification documents including passport and driving licence and information in relation to immigration status and right to work for us
- Information relating to disciplinary or grievance investigations and proceedings
- Information relating to performance and behaviour at work
- Training records
- Electronic information in relation to use of IT systems/swipe cards/telephone systems
- Images (whether captured on CCTV, by photograph or video)
- Vehicle details
- Any other category of personal data which we may notify the data subject of from time to time.

6.2 *'Special categories of personal data'* are types of personal data we may hold consisting of information as to:

- Gender; sexual orientation; racial or ethnic origin; religious or philosophical beliefs; genetic or biometric data; political opinions of opportunities
- Trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members
- Sickness absence, health and medical conditions to monitor ability to pay service charges, monitor absence from work, assess fitness for work, to pay benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after health and safety of clients and employees
- Any criminal convictions and offences

We may hold and use any of these special categories of personal data in accordance with the law.

6.3 *'Processing'* means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring or storage
- Adaption or alteration
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination
- Restriction, destruction or erasure

This includes processing personal data which forms part of a filing system and any automated processing.

6.4 *'Data subject'* refers to a living individual to whom personal data relates.

6.5 Data subjects can make a *'subject access request' (SAR)* to find out the information we hold about them.

6.6 Personal data must be processed in accordance with six *'Data Protection Principles.'*
It must be:

- Processed fairly, lawfully and transparently
- Collected and processed only for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed securely

We are accountable for these principles and must be able to show that we are compliant.

7. Related Legislation and Documents

Data Protection Act 2018 (the '2018 Act')
EU General Data Protection Regulation ('GDPR')