Data Protection Policy

Introduction

The processing of personal data is regulated by law in the form of the Data Protection Act 2018. This act is the United Kingdom's implementation of the General Data Protection Regulation (GDPR) which came into effect on 25 May 2018. This policy is designed to accommodate both the Act and the principles of GDPR.

Policy statement

Grand Union Housing Group collects and stores personal data about colleagues and our customers to ensure we continue to offer and provide the best services. We are committed to making sure we protect privacy which means we will:

- collect only relevant information
- only collect information that we need
- be transparent about why we collect it and how we'll be using it

Other laws that relate to the Act and GDPR include:

- Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- Data Retention and Investigatory Powers Act 2014
- Privacy and Electronic Communications Regulations 2003
- Computer Misuse Act 1990
- Human Rights Act 1998

Objectives

The processing of all personal data by Grand Union will only be undertaken in a fair, lawful and transparent manner, meaning:

- Fairness; no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person whose data is being collected. All privacy information, and any changes to privacy information, must be approved by the DPO.
- Lawfulness; no data collection activities will be undertaken or commissioned without there being a lawful ground for the data processing activities. Where legitimate interests are identified as lawful grounds, an assessment will be undertaken and documented. The data process owner is responsible for ensuring that lawful grounds are documented, consent is obtained, or the assessment is complete. The DPO will provide advice regarding lawful processing conditions.
- Transparency; we will endeavour to provide sufficient information about how personal data is being processed to enable sufficient transparency about its handling.

Other related policies

- Equality, Diversity and Customer Care Policy
- IT Use and Security Guidelines
- Mobile Device Guidelines
- Internet and Email Guidelines
- Data Protection and Security Breach Procedure

Policy details

How we process and manage data

Data minimisation

We will strive to use the minimum of personal data in processing activities and will periodically review the relevance of the information we collect. Data process owners are responsible for ensuring that no un-necessary, irrelevant or unjustifiable personal data is collected or created.

Data accuracy

We recognise that the accuracy of data is important, and that some data is more important to keep up to date than others. Data process owners will keep data as accurate and up to date as possible, in particular, data which would have a detrimental impact on data subjects if it is deemed inaccurate. Personal data that is assumed inaccurate will be dealt with appropriately through erasure or anonymisation.

Data retention

Personal data will not be retained for any longer than is necessary and for the purposes for which it is collected. Appropriate measures will be taken at the end of the data's useful life such as erasure to ensure this. Data process owners will be responsible for determining the retention period for personal data and update the Records of Processing Activities with end of life treatment.

Information security

Information security is contained within the IT Use and Security Guidelines. This gives detailed assurance that any personal data is held securely, confidentially, with integrity and is available.

Record keeping and accountability

In order to fulfil our responsibility to be able to demonstrate compliance with data protection legislation, we will maintain the Records of Processing Activities that we control, undertake or otherwise commission as required by the legislation and specifically those required in Article 30 of the GDPR.

Information rights

We recognise the legal rights of those whose personal data we are processing and will ensure that appropriate information is provided to them advising them of their rights:

- to information about data processing operations
- of access to personal data
- to portability of personal data
- of rectification of personal data
- of erasure of personal data
- to restriction of processing
- to object to direct marketing
- to object to data processing operations under some circumstances
- not to be subject to automated decisions under some circumstances
- of complaint about the processing of personal data and the right to a judicial remedy and compensation

Consent

We will interpret valid consent as defined in the GDPR if there is a genuine choice and;

- it has been explicitly and freely given by the data subject and they agree to the processing of personal data relating to them
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them
- we can demonstrate that the data subject has been fully informed about the data processing arrangements and we can prove that we have obtained valid consent lawfully

We will recognise that consent may be rendered invalid if any of the above criteria cannot be met. Consent is considered to not be forever, and we will determine a refresh period for every instance where consent is the lawful condition for processing.

There will also be processes in place to easily enable data subjects to withdraw consent and that the data subject is informed about how to exercise this right.

Personal/sensitive data breaches

We will maintain a Data Breach Reporting Procedure and will ensure that all colleagues, and those with access to personal data, are aware of it. All colleagues and individuals with access to personal data must report all personal data breaches to the Data and Information team as set out in the procedure as soon as they become aware of the breach.

Any other breach of this policy must also be reported immediately to the Data and Information team. Disciplinary action (including dismissal in a serious case) will be taken against any colleague depending on the scale of the breach. The person responsible for the breach may also be open to criminal proceedings; the result of which may be an unlimited fine or even a custodial sentence.

Data processing activities

We reserve the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with data protection legislation.

Data sharing, disclosure and transfer

We will only share personal data with third parties where there is a legal basis for doing so and data sharing is necessary for specified purposes. No sharing is permitted to occur without an 'Information Sharing Agreement' being in place. These agreements must be approved by a member of the respective Leadership team and stored in a central register.

The IT Use and Security Guidelines provides information and approved methods of transferring personal data to recipients. If this guidance is not followed, then disciplinary action will be taken.

Subject access requests (SAR)

Any person may ask Grand Union for the data that we hold or process about them. Any such request should be immediately passed to the Data and Information team for action. We must respond within one calendar month to any such request. Any data where the person making the request can be identified as the subject of the data has a right of access to this information. This data must be made available electronically to the subject.

From 25 May 2018 the SAR must be provided free of charge to the subject.

Sharing personal data outside the EU

We will neither transfer, process or permit personal data outside the EU without the conditions laid down in the data protection legislation being met. This will ensure that the level of protection of personal data is not undermined.

Risk assessments and impact assessments

When we are planning new processes or projects that involve the processing of personal data, we will carry out a Data Protection Impact Assessment (DPIA). This is to ensure that potential risks to individuals can be identified and addressed at the beginning of the implementation stage and data protection good practice can be built into the process.

We will embrace the principles and foster a culture of privacy by design. We will maintain a register of any completed DPIAs.

DPIAs will be conducted in accordance with the ICO's Code of Practice Conducting privacy impact assessments and the European Guidelines on Data Protection Impact Assessments.

The operational risk register will include a risk that covers data protection compliance and this will be reviewed quarterly.

Children's data

We will take special measures when processing personal or sensitive data relating to children under the age of thirteen including the nature of privacy information provided and approach to information rights requests.

Training and awareness

We will ensure that all our colleagues who engage in processing personal data are provided with appropriate training in this and our other associated policies and procedures. We will also undertake data protection awareness campaigns routinely to keep data protection front of mind. Formal refresher training will be provided to everyone at least annually.

Audit and compliance checking

We will undertake periodic compliance checks to test whether this policy is being adhered to and to test the effectiveness of control measures. Records will be kept of all such audits and compliance checks including corrective actions taken.

Action plan (if applicable)

N/A

Monitoring

The Executive Management team (EMT) is required to ensure compliance across the organisation with this policy.

Leadership team will be accountable for the management of data protection within Grand Union and the approval of minor changes to this policy.

Any complaints made relating to breaches or possible reportable breaches will be reported to EMT for investigation and recorded on the Data Protection log.

This policy will be monitored as part of the policy review programme.

Person responsible for review:	Director of IT
Supported by:	N/A
Ratified by:	Leadership team
Date policy reviewed:	February 2021
Date of next review:	February 2022