

Data Protection Policy incorporating the General Data Protection Regulation

Effective date: May 2018

Review date: May 2019

Approved: DSCF/ DLL board – May 2018

Author: Corporate Services Director

Version Control: 3.0

ICO registration number: ZA155775

CONTENTS	PAGE
Introduction	2
Objectives	3
Data Sharing	4
Data Retention	4
Individuals' right of access to data	5
Breaches	5
Policy promotion and training	6
Monitoring and feedback	6
Internal Personal Data	6
Glossary of Terms	6

1.Introduction

Dolphin Square Charitable Foundation (DSCF) and its subsidiaries (collectively known as Dolphin Living) controls and processes personal information about its customers, staff and board members. The UK's data protection approach has been amended following the adoption of the General Data Protection Regulation (GDPR) in May 2018. The principles of the new GRPR build up on the existing Data Protection Act 1998 (DPA) but the obligations are more extensive.

The GDPR covers all personal information that relates to living individuals. These individuals are given rights by the DPA and the GDPR. We will not share this information with other organisations without the consent of the individual concerned unless we are required by law to do so.

This Policy will set out what Dolphin Living will do to comply with the GDPR and the existing eight principles in the DPA.

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall only be obtained and further processed for specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose that they are processed.
4. Personal data shall be accurate and kept up to date.
5. Personal data shall not be kept longer than necessary.
6. Personal data shall be processed in line with the rights of the data subject.
7. Personal data must be kept secure.
8. Personal data must not be transferred to a country without adequate protection.

GDPR provides the following rights for individuals (Article 5):

1. The right to be informed
2. The right of access
3. The right of rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Being fair and understanding our customer's needs

We recognise that communities are made up of people with different needs and values and that those differences are important. We will promote equality of access for everyone and value their diversity. We will work to eliminate discrimination and, in line with the law, we will treat everyone fairly, regardless of age, disability, gender, reassignment, marital status including civil partnerships, pregnancy and maternity, race, religion or belief or sexual orientation. We will ensure that members of all these groups are treated in ways that meet their needs, and that they have equal access to services and/or activities wherever possible. We will promote their inclusion and challenge discrimination against them.

Scope

This policy applies to all employees, board members and others who may be involved in the collection of and processing of personal information on behalf of Dolphin Living and extends to data whether it is help on paper or by electronic means.

Partnership arrangements – where Dolphin Living work in partnership with external service providers this policy is applicable. Dolphin Living work with Touchstone, a managing agent, who provide the housing management service for all Dolphin Living's units. The introduction of GDPR places obligations on both 'controllers' and 'processors' in relation to maintaining and processing personal data.

Statement of commitment

Dolphin Living is committed to maintaining high standards of security and confidentiality for information in our custody and control. Safeguarding this information is critical to the successful operation of Dolphin Living. Dolphin Living will treat all information in its care and control with the same degree of security and confidentiality, and this Policy applies to all organisations within Dolphin Living and all its employees. Dolphin Living undertakes to inform residents, contractors, employees and board members on how it uses information and the purposes for which information is processed.

2. Objectives

The objectives of this Data Protection Policy are:

- To comply with the Data Protection Act 1998 (the Act) and any successor legislation to the Act.
- To comply with the European General Data Protection Regulation (GDPR), May 2018.
- To outline, guide and monitor the coordination of the information, security and data handling procedures in force within Dolphin Living.
- To promote confidence in Dolphin Living's information, security and data handling procedures.
- To provide assurances for third parties dealing with Dolphin Living.
- To provide a benchmark for employees on information, security, confidentiality and data protection issues.

Enablers

In order to support these objectives, Dolphin Living will:

- Delegate the responsibility of gathering and disseminating and dealing with issues relating to information, security, the DPA, GDPR and other legislation.
- Ensure that all activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information, security and compliance with GDPR and DPA.
- Ensure that all contracts and service level agreements between any part of Dolphin Living and external third parties (including contract staff), where personal data is processed, make reference to the GDPR where appropriate.
- Ensure that third parties acting on behalf of Dolphin Living are given access to personal information that is appropriate to the duties they are undertaking and no more.
- Ensure that all staff (including contract staff) and board members understand their responsibilities regarding data protection and information security under the GDPR.

3. Data Sharing

There are a number of occasions where it will be necessary for Dolphin Living to share personal data collected. Primarily personal data is shared and/ or disclosed to our managing agent, Touchstone, who delivered the housing management function of behalf of Dolphin Living.

Personal information is also shared with Local Authority partners when providing housing to referrals from their local housing lists or particular schemes. Under the GDPR Dolphin are required to explain to all individuals how they will use personal data which is collected and shared. This explanation is discussed with all incoming tenants as part of the tenancy sign up process.

All tenants are told –

- Who we are
- Why we are going to share personal data;
- Who we are going to share it with – whether a named organisation (Touchstone) or types of organisation; and
- In some cases where we have a duty to disclose information by law.

This policy ensures our processes for sharing is legal, how the accuracy of the data will be maintained and what security measures are in place prior to any sharing of information. It also provides the correct parameters of when it is appropriate to share and/ or disclose data. Dolphin Living have appropriate data sharing agreements (DSA) or similar with all parties which are reviewed on a regular basis and recorded on a central DSA log. Dolphin Living routinely share data with Touchstone to provide the housing management function. All decisions to share data are well founded, reflect the current needs of Dolphin Living and compliant under the requirements of the Act and GDPR. The contract confirms that Touchstone acts a Data Processor for personal data to perform the service or any other obligation. There are however exceptions in delivering the service where Touchstone are data controllers in their own right are responsible for any data breaches and associated liabilities for example, market tenanted properties. Dolphin Living remain the data controller throughout the contract to deliver the services and have overall control over the purpose for which, and the manner in which, personal data is processed and carry out data protection responsibility for it.

Exemptions

In some circumstances, it may be appropriate to disclose information held by Dolphin Living to specific third parties for example to prevent a criminal offence from being committed, or to prevent the continuation of a criminal offence.

4. Data Retention

Personal data must only be kept for the length of time necessary to perform the process for which it was collected. This applies to both electronic and non-electronic data. Data received from application forms or similar will be kept on file for up to 5 years after a tenant has moved out of a property. For applicants not eligible for housing following verification, all data records will be deleted immediately.

Under GDPR a new requirement is the right to be forgotten. Individuals can request deletion of certain types of information about them deleted where one of a number of circumstances apply:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child

Disposal

Where personal and confidential information is no longer required, it will be destroyed.

Privacy notice

A privacy notice is published on Dolphin Living's website outlining how we use information collected, how long personal data is kept for and what lawful basis Dolphin Living have to process data. The notice also includes tenant rights to request access personal information.

5. Individuals' rights of access to data (Subject Access Requests (SARs))

Individuals have a right of access to personal information held by Dolphin Living if they are the "data subject" of that information. Requests must be made in writing, signed by the data subject and addressed to the Head of Corporate Services. The person requesting the data must complete the [Subject Access Request Form](#) providing details of the information required as well as their current address and some form of identification. There is no charge for responding to the request. In those rare cases a data controller may choose to refuse the request entirely. Timescales for responding to a SAR should be without undue delay or within 30 days.

Where a SAR is made electronically, the information should also be provided electronically unless the individual requests otherwise. Where possible Dolphin Living should consider providing individuals with direct and remote access to their data through a secure system. As well as providing copies of the relevant data, Dolphin Living must provide further explanatory information about the way in which the information is used, who it will be shared with, how long it will be kept, and information on the rights to rectification, erasure, and to complain to the ICO.

Someone may ask a third party to obtain the information on their behalf, but they must provide written consent in order to do this.

If a SAR is received directly or indirectly the responsibility for responding will be assigned to the Customer Services Manager. The Corporate Services Director will ensure the SARs are processed efficiently and in accordance with GDPR; and ensure the documented process has been approved by senior management and made readily available to personnel.

6. Breaches

Dolphin has appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. Dolphin Living has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage e.g. through identity theft or confidentiality breach. In the case of a personal data breach, Dolphin Living shall without undue delay and, where feasible, no later than 72 hours after becoming aware of it, notify the breach to the ICO. There are also appropriate mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

Regular data mapping and appropriate contact relations management system ensures that Dolphin Living are aware and action any breach of data in an appropriate manner.

Any wilful disregard or intentional breach of the Policy by employees shall be regarded as a disciplinary offence and handled within Dolphin Living's Disciplinary Procedures. Any wilful disregard or intentional breach of the Data Protection Policy by data processors (and identified data controllers in their own right) acting on Dolphin Living's behalf under contract shall be regarded as a breach of contract and treated as such.

Equality impact assessment ('EIA')

After completing a Stage 1 EIA, it was found that this policy will affect all employees and residents in the same way as all personal data should be processed in accordance with the GDPR. As long as any data requested is made available in a way that is suitable for the needs of the data subject, there will be no adverse impact on any particular group.

7. Policy promotion and training

The Policy will be available to all Dolphin Living employees and form part of the induction process to all new and temporary employees and board members. The policy is also available to prospective and current Dolphin tenants upon request or can be located on the Dolphin Living website.

The Policy will be promoted to current employees by requiring acknowledgement and acceptance of its aims and objectives. There will be a continuing series of awareness raising initiatives relating to security and privacy issues by the Data Protection Champions nominated around Dolphin Living in order to ensure that all staff understand their responsibilities under GDPR.

All employees will be provided with education and training where appropriate and will be expected to comply with data protection legislation and adhere to the policies and procedures used to meet the objectives of the Policy. Training will be refreshed on annual basis to all staff.

8. Monitoring and feedback

This policy will be monitored by the Corporate Services Director. It will be reviewed periodically as set out above capturing best practice, customer feedback and any legislative changes.

The Corporate Services Director is responsible for all data compliance and monitors Dolphin's approach to Data Protection.

9. Internal Personal Data

Dolphin Living maintain appropriate technical and organisational processes and procedures to safeguard against any unauthorised or unlawful processing of personal data. Data audits are carried out annually to monitor the information we hold on employees, including former employees. For the purposes of HMRC compliance, financial information is held for 7 years and then destroyed. All HR files relating to former employees are kept up to a year after leaving the employment of Dolphin Living. After one year, all personal data Dolphin Living holds will be reviewed. Enough data to enable Dolphin living to deal with, say, providing references will be retained.

10. Glossary of terms

Personal Information/ Data – any information that relates to a living individual who can be identified by this data. Under GDPR, personal data includes information relating to a living person, who can be identified directly or indirectly by such information (e.g. name, ID number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic or social identify of that person). This includes opinions about the

individual and an indication of the intention of Dolphin Living or any other person in respect of the individual.

Data subject – the living individual that the personal data is about.

Data Controller – the company that decides the purpose for and the way in which any personal data is processed. Dolphin Living and certain of its subsidiaries are data controllers.

Data Processor – any company that carries out activities with personal data on behalf of the data controller.

General Data Protection Regulation (GDPR) – is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).

Sensitive Personal Data means personal data consisting of:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or other beliefs
- Whether they are a trade union member
- Their health including physical or mental condition
- Their sexual life
- Criminal proceedings or convictions
- Genetic data
- Biometric data
- Data concerning sexual orientation

Confidential information includes but is not limited to:

- Financial information
- Pricing information
- Administration and information systems
- Information about Grainger's tenants, customers, suppliers and trade connections, and its employees (including contractual details, remuneration and bonus figures of employees).

Data can be information, covering both facts and opinions held on:

- Computer
- Paper records
- Any accessible record (e.g. e-mail, electronic device)