CS012 – Data Protection Policy

MONITORING FORM	
Department	Corporate Services
Department Director	Chief Executive
This policy is applicable to	All Staff, Board, Tenants and other relevant stakeholders
Author	Human Resources Director
Original Version approved by & date	6 June 2018
Date of last review	6 June 2018
Version number	V3
Date of minor modification	12 February 2019
Period of Review	2 years
Date of next review	12 February 2021
Internal /external consultees (if required)	n/a

1. INTRODUCTION

This Policy sets out the statement of intent that Weslo Housing Management (WHM) staff will follow with regard to The General Data Protection Regulations (GDPR) to ensure compliance.

Its purpose is to protect the "rights and freedoms" of natural persons (e.g. living individuals) and to ensure that personal data is not processed without their knowledge and wherever possible, that it is processed with their consent.

It aims to ensure that those who record and use personal information are open about the use of that information and develop sound and reasonable practices in its operation.

Weslo Housing Management (the company) recognises the importance of the guiding principles of GDPR in terms of protecting the rights of individuals in respect of personal information that is kept about them in any form.

2. SCOPE

For the purposes of this policy it is deemed to include the following: Weslo Housing Management and its subsidiary, Weslo Property Management, Board Members, all employees (permanent, temporary or contracted) and any other stakeholder if relevant to the Policy.

WHM and WPM are registered with the Information Commissioner's office for the purpose of Data Protection. Registration numbers are Z4942310 and ZA0292223 respectively. As such we will ensure the information provided to us will be treated in confidence and in compliance with the Data Protection Act.

3. BACKGROUND

GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means (e.g. paper records) that form part of a filing system or are intended to form part of a filing system.

Weslo will only store information within the UK and EEA**.** Should personal information be stored out with the UK and EEA, Weslo will ensure that there are adequate safeguards in place to protect your information in accordance with this notice, including the following:

- Decision made by the Information Commissioners Office that the third country has adequate safeguards in place;
- Procedures are outlined to 3rd parties regarding their use, storage and disposal of information;

4. DEFINITIONS & EXPLANATIONS

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. It also includes Children with a child being defined as a person under the age of 16. The processing of information relating to a child is only lawful if parental or custodial consent has been obtained.

Data controller – means a person who (alone, jointly or in common with other persons) determines the purpose for which and the manner in which personal data will be processed. For example: we control the information added to the Housing Management Information System used to manage tenancies.

Data processor – means any person (other than an employee of the controller) who processes the data on behalf of that controller. For example: Third parties used to facilitate mailshots.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

5. GDPR PRINCIPLES

The GDPR contains 7 principles which regulate the way personal data can be collected, handled and used. Weslo will adopt and operate procedures in accordance with the GDPR Principles ensuring all personal data and information held is:

a. Obtained and processed transparently, fairly and lawfully [GDPR Principle 1 - lawfulness, fairness and transparency] ;

b. Obtained only for specified and lawful purposes, and shall not be used for any other purpose [GDPR Principle 2 - purpose limitation];
c. Be adequate, relevant and limited to what is necessary for processing [GDPR Principle 3 - data minimisation]
d. Be accurate and up to date with every effort to erase or rectify without delay [GDPR Principle 4 - accuracy];
e. Be held no longer than is necessary for the purpose for which it is collected; [GDPR Principle 5 – Storage Limitation]
f. Be processed in a manner that ensures the appropriate security [GDPR Principle 6 - – integrity and confidentiality]
g. Be able to demonstrate compliance with the GDPR's other principles [GDPR Principle 7 –accountability

6. LAWFUL BASIS

Weslo, and all staff who use any personal information, must ensure that they follow the seven Principles as outlined above and also take into account the six lawful reasons for processing information as set out in Article 6 of the GDPR, detailed below. It should be noted that at least one of these must apply whenever personal data is processed:

- **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for us to have a contract with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for our 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.

All processes within Weslo which involve the gathering, processing, storing and sharing of personal data has been recorded on a Data Inventory which are held centrally by Corporate Services. Managers are responsible for ensuring that these inventories are kept up to date when there are changes to procedures or new processes/projects are undertaken.

We recognise there will be a need to share some personal data in order to deliver services, perform our duties and legal obligations but will only do so where we have permission or a legal power to do so. We will provide notices which explain why we collect personal information and how we use and share information these can be found on the company intranet and Website.

7. CREATING, STORING AND MANAGING INFORMATION

Staff at Weslo will:

- process and keep personal and confidential information safe and secure at all times, including at the office, public areas, home or in transit. Such information will not be divulged or discussed except in the performance of normal work duties.
- classify and use information according to its risk, sensitivity, value and importance while considering who should receive or have access to it.
- use our policies and procedures for assessing information risk.
- only store information in approved locations and methods, networks, systems, paper archives or devices as appropriate.

7. GIVING ACCESS TO INFORMATION

Staff must respect people's right to access personal and public information that Weslo creates, owns or holds about them and assist them in accessing it.

7a. Subject access requests

Individuals have the right to make a subject access request which should be referred to Corporate Services where the Subject Access Request Procedure will be applied.

Individuals have a number of other rights in relation to their personal data. They can require Weslo to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override the Weslo's legitimate grounds for processing data (where Weslo relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override Weslo's legitimate grounds for processing data.

To ask Weslo to take any of these steps, the individual should send the request to corporate.services@weslohm.co.uk

7b. Disclosing Personal Information

Weslo must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.
All employees should exercise caution when asked to disclose personal data held on another individual to a third party.

It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Weslo's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the line manager.

Staff must follow Weslo Housing Management's policies and procedures for sending and sharing personal and confidential information outside the business including use of secure email and encryption for sending electronic information. Staff must also follow sharing protocols when a 'sharing agreement' is in place. [Refer to

7c. Retention, Preserving and Disposing of Information

Weslo Housing Management will only retain information for the time period applicable to the purpose for which that information was obtained as outlined in our Retention Schedule.

This will apply to both paper and electronic formats. Some information will be kept for longer periods than others, however every effort will be made to review the need to keep it and safely dispose of data as soon as possible. For information that is deemed worthy for historic or research purposes we must be able to evidence that there is a genuine business reason why this information should be retained indefinitely.

7d. CCTV

Where CCTV is in use images will be treated as "data" in the same manner as paper or computer based information.

The main purpose of collecting data from CCTV cameras is the protection of Weslo's employees, tenants and the public, the prevention of crime or anti-social behaviour and to safeguard Weslo's property.

Data from CCTV cameras may be used as evidence during criminal or other legal proceedings and may be passed to agencies within the scope of our Policy and with the guidelines set by the Information Commissioner. Recording images will be kept securely and accessed by authorised personnel.

CCTV will not be located in a position where images can be seen by members of the public.

Proper warning signs will be displayed in all areas covered by CCTV. The signage will detail the purpose of use, who is responsible for operating the system (Weslo) and who to contact (telephone number) in the event of an enquiry

CCTV images are the property of Weslo Housing Management.

8. IF THINGS GO WRONG – REPORTING A BREACH

A Data Protection Breach can happen for a number of reasons and can be related to:

- Loss or theft or data or equipment on which data is stored;

- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Data Breaches must be reported to the Information Commissioners Office within 72 hours.

Should a breach occur it is vital to ensure it is dealt with immediately in accordance with our Data Protection Breach Procedure to minimise the impact of the breach and to prevent a reoccurrence.

Staff should report the breach or a potential breach to Corporate Services as soon as they become aware that a data protection breach has occurred.

In order to allow Corporate Services to manage the situation, the staff member must complete and the Data Protection Breach Notification Form and send this to Corporate Services at the time of notification. Upon receipt of the form, Corporate Services will then take the necessary steps to manage the breach in accordance with the relevant procedure.

9. DATA INVENTORY

Weslo has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. The data flow and inventory is held centrally by Corporate Services and contains the following:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- any data transfers ; and
- all retention and disposal requirements.

DATA PRIVACY RISK ASSESSMENT

10. GDPR TRAINING

All staff will have access to appropriate and relevant training to ensure compliance and an understanding of GDPR.

11. RESPONSIBILITIES

11.1 Executive Team

The Executive Team are responsible for developing and encouraging a culture that is committed to ensuring compliance with GDPR and adherence to our overall Information Management Framework.

11.2 Management Team

All managers are responsible for the implementation and monitoringof this policy, associated policies, standards and procedures within their service area.

11.3 Corporate Services

Corporate Services are responsible for:

- Implementing the requirements of Data Protection
- Notifying, registering and liaising with the Information Commissioner hem should a breach occur;
- Co-ordinating any amendments to our registration;
- Monitoring and reporting to the Executive Team on compliance and any subject access requests;
- Carrying out Data Impact Assessments, liaising with relevant Managers for areas for improvement, monitoring reviewing agreed actions;
- Coordinating Subject Access Requests [SAR's] and being the first point of call for clarification on any aspect of data protection compliance;
- Advising line managers on Data Protection and delivering relevant data protection training for all employees.

11.4 All Staff

11.4.1 All staff have a responsibility for adhering to this Policy and any associated policies, standards and procedures that support the Policy and our overall Information Management framework.

11.4.2 Individuals are responsible for helping Weslo keep their personal data up to date. Individuals should let Weslo know if data provided changes, for example if an individual moves house or changes his/her bank details.

11.4.3 Individuals who have access to personal data are required to:

- only access personal information that is necessary for their role and business need.
- dispose of paper and electronic information classified as personal or confidential as per our retention schedule.

- not disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- keep their individual accounts and their user name and passwords for their own use and not share these with others
- make use of strong passwords that conform to the minimum standard, when accessing system accounts, applications and encrypted devices and must not disable password protection standards.
- lock computer screens on any devices or log-out/shut down before leaving any workstation or device.
- take all reasonable precautions to keep all Weslo supplied mobile/portable computing equipment safe and secure when taken out of the premises.
- only use Weslo's registered assets (hardware, software, applications and services) that are approved for Weslo business to ensure information risks are assessed, confidential information is secure and the assets are all registered.
- Ensure ICT guidelines are followed to ensure unauthorised access to Weslo equipment or knowingly introduce any security threat
- not to store personal data on local drives or on personal devices that are used for work purposes;
- ensure all Weslo information and equipment they own or hold is transferred or returned to ICT before leaving Weslo.
- report data breaches of which they become aware to corporate services immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal.

12. RISK MANAGEMENT

The Company has considered the risks of the storing of personal information and recognises the possible consequences should we fail to adhere to the principles within the Act. These include:

- being enforced to bring our practices in line with the Data Protection Act;
- being prosecuted by the Information Commissioner if a criminal offence has been committed, such as unlawfully obtaining personal data;
- being required to give compensation to an employee through the courts if damage has been caused by our failure to meet the Act.

Information Compliance and Data Protection has been identified as a risk and as such will be monitored through our Risk Management Register. It forms part of our governance structure and will be part of our Internal Audit Review Cycle.

Weslo is aware of any risks associated with the processing of particular types of personal data.

Weslo assesses the level of risk to individuals associated with the processing of their personal data by carrying out a Data Protection Impact Assessment [DPIA] in relation to processing undertaken by other organisations on behalf of Weslo.

Weslo shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Weslo shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA it is clear that Weslo is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Weslo may proceed must be escalated for review to the Executive Team.

The Executive Team shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

Appropriate controls will be selected [from Annex A of ISO 27001, ISO 27017, ISO 27018, etc., as appropriate] and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Organisation Name's documented risk acceptance criteria and the requirements of the GDPR.

13. EQUALITY & DIVERSITY

This Policy will always be carried out in accordance with Weslo's Policy of Equality & Diversity which aims to promote diversity, fairness, social justice and equality of opportunity by adopting and promoting fair policies and procedures.

14. PUBLICISING AND AVAILABILITY

This policy is available on the Weslo website, to Board, staff members and any other key stakeholders. Copies are available free of charge. A summary of this policy can be made available in other formats and languages.

15. MONITORING & REPORTING

This policy will be reviewed every two years to ensure compliance with applicable legislative changes, changes within the organisation and best practice.

16. COMPLAINTS

Anyone wishing to make a formal complaint should do so as per our complaints procedure.

17. OTHER RELEVANT DOCUMENTS

A suite of documents, policies, procedures relevant to GDPR have been compiled by Corporate Services and include, Fair Processing Notices (FPNs), Privacy Statement, Subject Access Request Procedure and forms, , CCTV Procedure, Complaints Procedure, Data Impact Assessment Procedure, Breach Procedure, Data Sharing Agreements, Processing Agreements, Photography Consent and Withdrawal of Consent Forms, etc. These can be found on the Intranet.