Victorguard Care

POLICY NO: 107

DATA PROTECTION POLICY

The Policy defines the arrangements in place within Victorguard Care PLC that assures compliance to the requirements of General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018), as relevant to the Home's business interests:

1. INTRODUCTION

GDPR, 2018 addresses certain requirements for all businesses that collect (control), process personal data as a part of their on-going business operations and who have day-to-day responsibility for data protection.

Victorguard Care PLC is data controller and data processor under GDPR.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

2. PRINCIPLES OF DATA PROTECTION

Under the GDPR, the data protection principles set out the main responsibilities for organisations as following:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

Victorguard Care PLC as a data controller is required to be responsible for, and be able to demonstrate, compliance with the principles above.

3. POLICY DETAILS

3.1 Victorguard Care PLC collect and process personal data on a valid lawful basis as following:

- Consent:
  - ✓ freely given;
  - ✓ obvious and require a positive action to opt in;
  - ✓ cover the controller's name, the purposes of the processing and the types of processing activity;
  - ✓ no set time limit for consent – regularly reviewed;
- Legal obligation:
  - ✓ process the personal data to comply with a common law or statutory obligation;
  - ✓ collecting and processing must be necessary;
  - ✓ the individual has no right to erasure, right to data portability, or right to object
- Legitimate interests:
  - ✓ use personal data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing;
  - ✓ processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;

3.2 Special category data are collected and processed on following conditions only:

- ✓ the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- ✓ processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is

3.3 Criminal offence data

- Victorguard Care PLC does not collect or process any Criminal offence data; Legal duty is the DBS check only, what requires ID check and prove of address, but we do not keep any copies of these documents; Company collects and process the DBS date and number to comply with CQC expectations.

3.4 Individual rights:

- Right to be informed - Individuals have the right to be informed about the collection and use of their personal data;
- Right to access - individuals have the right to obtain a copy of their personal data as well as other supplementary information. Company arrange the employee to see or hear all personal data held within 30 days of receipt of a written request. For a hard copy Company may request the £10.00 administration fee;
- Right to rectification - Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data
- Right to erasure - Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances
- Right to restrict processing - Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.
- The right to data portability - gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller.
- Right to object - Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.

  The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.

- Rights related to automated decision making including profiling – Victorguard does not use any automated decision-making systems;

3.5 Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure. Records can be hard copy (paper) format and computer files. In each case particular attention is paid to the following aspects of record storage.

- Hard Copy (paper) files:
  - ✓ Location of storage – locked rooms and/or locked cabinets;
  - ✓ Identification of those employees authorised to have access;
  - ✓ Responsibilities for secure storage;
  - ✓ Retention times;
- Computer files
  - ✓ Responsibilities for implementing security systems for computer files;

- ✓ Password protection for access to sensitive data files;
- ✓ Who is authorised to have knowledge of these passwords;
- ✓ How often passwords are changed;
- ✓ Implications for network systems;
- ✓ Records retention time;
- ✓ Back-up, control and management of what are essentially copies of personal data;
- ✓ Antivirus, antispyware software implemented
- ✓ Remote access in emergency, under DPO & IT specialist supervision;

- when personal data are being processed, administrative staff will take all reasonable precautions to prevent sighting of data by unauthorised persons:
  - ✓ record files are locked away when not in use;
  - ✓ where practical, computer display screen should be tilted towards the user and away from the general office environment;
  - ✓ VDUs are not left on when not in use;

4. PURPOSES & TYPE OF DATA COLLECTED AND PROCESSED

- For list of data and purposes please see appendix 1 (Information Mapping);

5. RESPONSIBILITY FOR THE COLLECTING AND PROCESSING OF PERSONAL DATA

- The company will appoint The Data Protection Officer as the named individual responsible for ensuring all personal data is controlled in compliance with GDPR;

Policy date: ……..

Authorised signatory: ……..

Policy revive date: ……..