Heritage Care at Home Ltd
Data Protection Policy
Policy reviewed and valid from: 01/01/20

INTRODUCTION

Personal data is used throughout Heritage Care at Home Ltd as part of normal day-to-day business. This policy sets out how Heritage Care at Home Ltd will meet its legal obligations under the Data Protection Act 1998 ("the DPA") and to protect the confidentiality of sensitive personal information in light of guidance from the Department of Health.

The DPA applies to all personal data held in filing systems, contact databases, emails, and portable media. It includes any information that can be used to identify a living individual such as photographs, contact names and addresses for staff, stakeholders, and others with whom we do business. It also includes information processed on behalf of Heritage Care at Home Ltd by third parties.

Heritage Care at Home Ltd regards the lawful and correct treatment of personal information as essential in order to protect the interests of those whose personal data we hold and to maintain confidence in our operations. Accordingly, Heritage Care at Home Ltd will ensure that all personal information will be processed in accordance with the Data Protection Act 1998 and guidance from the Department of Health.

The Data Protection principles

Heritage Care at Home Ltd will adhere to the principles of the General Data Protection Regulation which require that personal information is:

- 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.
- Heritage Care at Home Ltd will comply with the relevant GDPR procedures for international transferring of personal data.

Definitions

Personal data is defined in the Act as any information that "relates to a living individual who can be identified from:

- those data
- those data and other information which is in the possession of, or is likely come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual"

This definition should be considered in light of the extent to which the data relates to the individual's privacy in their family life, business or professional capacity. In particular, consideration should be given to whether the information is biographical in a significant sense, or whether it has the individual as its focus.

The Department of Health has advertised that "sensitive personal data" is information that includes the name of an individual **combined with** one or more of the following:

- Bank / financial / credit card details
- National Insurance number / Tax, benefit or pension records
- Travel details
- Passport number, information on immigration status or personal (non-Heritage Care at Home) travel records
- Health records
- Work record
- Material related to social services (including child protection) or housing casework
- Conviction / prison / court records / evidence
- Other sensitive data defined by the Data Protection Act 1998 including information relating to a person's:
  a) racial or ethnic origin
  b) political opinions
  c) religious beliefs or other beliefs of a similar nature
  d) membership of a trade union
  e) physical or mental health or condition
  f) sexuality
  g) the commission or alleged commission by an individual of any offence
  h) any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings

Responsibilities
The Directors have overall responsibility for data protection within Heritage Care at Home Ltd. The Registered Manager is responsible for day-to-day corporate compliance with the Data Protection Act and providing advice to staff.

Management of personal data
Personal data should only be collected where it is necessary for the work of Heritage Care at Home Ltd and should be kept to the minimum necessary for the task. Staff should follow good practice for handling personal data as set out in the data protection Good Practice Guide. In particular:
Heritage Care at Home Ltd will only use personal information where this is necessary to carry out its functions

- Personal data will be anonymised where it is not necessary to identify the individual for the stated purpose
- Information solicited in response to website or other consultations will include an appropriate data protection statement at all gateways
- Portable media that may contain personal data will be encrypted if held outside secure office premises based on a risk assessment
- Sensitive personal data will not be published on Heritage Care at Home Ltd's website with the exception of personal testimonies where the individual has provided explicit written consent
- All records containing personal data will be destroyed in accordance with Heritage Care at Home Ltd's records retention and disposal schedules.

Security of sensitive personal data
Sensitive personal data must not be transported outside secure office premises on portable media (e.g. a laptop, memory stick, CD or DVD) unless the media is encrypted or password protected. All bulk transfers of other personal data, such as mailing lists, must be encrypted / password protected prior to transfer to third parties. Sensitive personal data sent by post should be marked 'confidential'.

All sensitive personal data held in office premises such as personnel records or unsolicited medical information contained in general enquiries must be kept securely in locked cabinets and offices, and only made available to authorised staff and third parties on a need-to-know basis. Access to sensitive personal data held in electronic form must be limited to a need to know basis and managed via appropriate permissions access on the Heritage Care at Home Ltd network.

Everyone managing and handling personal information is responsible for following good data protection practice in accordance with Heritage Care at Home Ltd's policies and guidance. Any potential breach of security concerning loss, inappropriate disclosure or misuse of sensitive personal data such as through lost or stolen laptops must be reported to the Registered Manager as soon as possible in accordance with the Incident Reporting Procedure.

Sharing personal data

Personal data may be shared with third parties where this is necessary for the performance of Heritage Care at Home Ltd's functions and in accordance with guidance from the Information Commissioner's Office.

Disclosure of personal information under FOI

In response to requests under the Freedom of Information Act ("the FOI") Heritage Care at Home Ltd may disclose staff personal data. On doing so it will give due consideration to whether in all the circumstances the disclosure would be fair to the individual and balance its duty of care to staff in respect of protecting their personal information from unwarranted intrusion with its legal obligations to disclose information under FOI.

When handling FOI requests for personal information there will be a presumption in favour protecting personal privacy:

- No HR information will be disclosed except in response to a subject access request
- No personal email address, direct fax or DDIs will be disclosed
- No names of staff will be disclosed except where they are in 'public facing roles
- Public roles are those where individuals deal directly with the public and where there is a legitimate expectation that their name should be known
- Job titles of staff will generally be disclosed
- Names of only Directors will be disclosed
- No private addresses will be disclosed

In applying this 'default' position it is recognised that names and contact details of some details of some staff are proactively placed in the public domain on the Heritage Care at Home Ltd website. Any such publicly available information will be disclosed.

Subject access requests

Any individual, including a member of staff, has a legal right of access to their personal data held by Heritage Care at Home Ltd under the Act. The Office will be responsible for managing all subject access requests by the public within statutory periods including verification of the identity of the individual.

Contracts

All contracts with third parties that involve the processing of personal data will include specific obligations to comply with the Data Protection Act 1998 and standard Office Government Commerce contract clauses on security / Information assurance where applicable.

Related policies

- Email and Internet policy
- Incident reporting procedure
- Secure Storage, Handling, Use, Retention & Disposal of Disclosures and Disclosure Information

Guidance on breaches of security for personal data

Breaches of security can occur for a number of reasons such as loss or theft of equipment, documents left on train or at meetings, simple human error or even hacking attacks. Data security breaches should be reported so that an assessment of the risks can be carried out and remedial action taken as necessary.

This guidance only applies where there is an actual or potential loss, misuse or disclosure or sensitive personal data as defined in above. It does not apply to information readily accessible in the public domain such as business names and addresses. If in doubt, the event should be reported.

When there is a breach of security, the following information should be reported to the Directors or Registered Manager as soon as possible:

- When the event occurred
- The type and quantity of sensitive personal data involved
- The circumstances of the loss e.g. theft from car, left on train
- Whether the breach is thought to arise from a systemic failure
- Description of the media containing the data such as laptop or memory stick
- What security was in place e.g. encrypted laptop, locked car
- Any other information considered relevant

Immediate remedial action depending on the risk involved. An incident report should be completed by the responsible manager, which may be included in the risk register and reported as necessary.