Policy: Data Protection

Policy Summary

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 requires data controllers and data processors to protect that data from causing harm to living individuals, and to demonstrate respect for people. The Hospice is committed to processing data in accordance with all current data protection regulations.

1. Scope

This policy applies to all data processed by employees and volunteers of Blythe House Hospicecare.

2. Rationale

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU), and fully adopted by the UK.

The General Data Protection Regulation (GDPR) and the Data protection Act 2018 introduced new elements to the data protection regime, superseding the Data Protection Act 1998. It requires organisations to be transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purpose of keeping adults and children safe. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk

3. Principles

3.1 The impact of our diverse population and our employees and volunteers has been reviewed and consideration has been given to the potential for each policy to lead to inequalities for people with protected characteristics, as defined by the Equality Act 2010 and to any possible measures to mitigate or remove potential inequalities. Protected characteristics are age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity.

3.2 **There are six data protection privacy principles:**

3.2.1 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals (fairness, lawfulness and transparency);

3.2.2 Personal data shall be 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 ('purpose limitation');

3.2.3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

3.2.4 Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that any personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

3.2.5 Personal data shall be 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 (storage limitation).

3.2.6 Personal data shall be 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 (integrity and confidentiality).

4. Duties

4.1 The Chief Executive Officer and the Data Protection Officer are responsible for notification of the Hospice's data holdings to the Information Commissioner's Office.

4.2 Managers must ensure that employees and volunteers are aware of and adhere to this policy.

4.3 Employees and volunteers must process data in accordance with this Policy and the Data Protection Guidelines (Appendix 1).

4.4 All data protection breaches must be reported and recorded in-line with the hospice Incident form.

5. Policy

5.1 The Hospice will conform to the regulations and principles of the Data Protection Act 2018. It will also recognise NHS and professional bodies' guidelines and protocols, particularly those arising from the Revised Caldicott Principles (2016) and HSC 1999/012. The Chief Executive Officer is the designated Caldicott Guardian for the organisation.

5.2 Data must be processed in accordance with the GDPR and Data Protection guidelines 2018 (Appendix 1) which list the types of data the Hospice is registered to process, the use that can be made of such data and the circumstances in which it may be disclosed.

6. Definition of Terms Used:

Caldicott Guardian: the person responsible for ensuring that national guidelines and protocols on the handling and management of patient information are in place. Within Blythe House Hospicecare the Caldicott Guardian is the C.E.O.

Data Protection Officer: the person responsible for monitoring all Hospice GDPR and Data Protection Bill compliance, with specific support to the Caldicott Guardian. Within Blythe House Hosicecare the Data protection Officer is Louise Furmston.

Data controller: the person, or institution, who is responsible for the manner in which any personal data is processed. The Hospice is the Data Controller.

Data Processor: any authorised individual or institution who process data on behalf of the Hospice including the Hospice itself.

Data Subject: a living individual who is a subject of personal and sensitive data collection

Confidentiality Clause: a clause included in the contracts of all employees and bank workers, requiring them to maintain the confidentiality of any relevant information that they come into contact with in the course of their work, e.g. information that is personally, clinically or commercially sensitive. There are separate confidentiality documents that volunteers, contractors and other third parties are required to sign, requiring them to maintain the confidentiality of such information.

Data: information about an identifiable living individual that is recorded

- on computer, or in an automated system
- in an indexed filing system, or
- with the intention of going into one of these systems.

Personal data: relates to a living individual who can be identified from the data, includes any expression of opinion about the individual and any indication of intentions of the Data Controller in respect of the individual. Note that this includes photographs and e-mail messages. It also covers data identified by reference numbers where a separate list can be used to match the reference numbers to named individuals.

Processing: obtaining, recording or holding the data, or carrying out any operation on the data, including organising, adapting or altering, retrieval, consultation, use, disclosure, erasure or destruction of the data

Sensitive personal data: includes personal data consisting of information such as:

- the racial or ethnic origin of the data subject
- their political opinions
- their religious beliefs
- whether they are a member of a trade union
- their physical or mental health
- their sexual life
- their gender
- the commission or alleged commission by them of any offence
- any proceedings for any offence committed or alleged to have been committed by them
- finance
- sickness
- biometrics (e.g. facial/fingerprints/iris recognition systems).

: **8. Supporting documents**

8.1 The policy standards will be met through working procedures, protocols, guidance, standards.

8.2 The supporting documents will not form part of the policy but are listed below and can be found under the Policy and Procedure electronic file on the hospice's public drive.

8.3 List of supporting policies

- Confidentiality Policy
- Information Governance Policy
- Record Management Policy

Appendix 1

Data Protection Guidelines

1. The Hospice is registered for the following categories of data:

1.1 Administration - refers to employee and volunteer data. The Hospice processes data about its staff, mainly through Administration staff, but also through other departments such as Volunteer and Support Services, Finance, Line Managers.

- Throughout employment and for as long a period as is necessary following the termination of employment, the Hospice will need to keep information for purposes connected with an employee's employment, including recruitment and termination information.
- The information held will be for our management and administrative use only, but from time to time, we may need to disclose some information we hold about employees to relevant third parties, e.g. where legally obliged to do so by HMRC or requested to do so by an employee for the purposes of giving a reference. We may also transfer information to another Group or Organisation, solely for purposes connected with an employee's career or the management of the Hospice's business.
- It should also be noted that the Hospice might hold the following information about an employee for which disclosure to any person will be made only when strictly necessary for the purposes set out below:

    1. an employee's health, for the purposes of compliance with our health and safety and our occupational health obligations
    2. for the purposes of personnel management and administration, for example to consider how an employee's health affects his or her ability to do his or her job and, if the employee is disabled, whether he or she requires any reasonable adjustment to be made to assist him or her at work
    3. the administration of insurance, pension, sick pay and any other related benefits in force from time to time
    4. in connection with unspent convictions to enable us to assess an employee's suitability for employment.

- The Hospice requires all employees to comply with the current GDPR and Data Protection Act in relation to the information about other staff. Failure to do so, e.g. unauthorised, inappropriate or excessive disclosure of or obtaining information about individuals, will be regarded as serious misconduct and will be dealt with in accordance with the Hospice's Disciplinary Policy and Procedure.

1.2 The Hospice processes data about its clients, through the Day Services, Hospice at Home team, and through the Clinical Departments, Macmillan Information and Support Services, Counselling and other departments.

- no personal detail about any patient, their family, past and present employees and volunteers or donors may be disclosed without proper authority. However, the duty to share patient identifiable information can be

as important as the duty to protect patient confidentiality (Caldicott Principle 7). If you are not sure whether to divulge information, please refer the request to your manager or seek the advice of the Caldicott Guardian, or the Data Protection Officer.

- GDPR and Data Protection Act (DPA) 2018 are not barriers to justified information sharing. Information that is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal. The DPA 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows hospice staff to share information without consent.
- all personal data must be protected from unauthorised access by lock or password.

1.3 Fundraising - refers to Donor data. The Hospice processes data about its donors, mainly through the Fundraising and Retail Departments.

1.4 Realising the Objective of a Charity - refers to external data subjects. The Hospice processes data about external data subjects who may or may not have direct links with its employees or volunteers. The data usually comprises contact lists of names and addresses for mailing and other purposes. For instance, Finance holds details of suppliers, Administrative staff hold details of training providers and Volunteer and Support Services holds details of contractors.

1.5 Research data. Hospice employees may process personal data as part of their research activities. This is likely to consist of responses to surveys which are then made anonymous for research purposes. Thus the data will usually consist of contact data and survey data. Such data is covered by the GDPR and its data protection principles. In some instances the data collected will come under the heading of sensitive data which may identify the subject. Any research or studies using patient records must be approved by a Local Research Ethics Committee or approved and / or requested by the Care Quality Commission. This means that explicit consent must be obtained from the data subject at the point of collection.

1.6 Photographs. Where photographs are taken within the Hospice careful consideration should be given as to whether the intended use of such photographs could render them personal data within the GDPR. If there is any doubt as to whether the intended use could be construed as use of personal data, prior consent must be obtained from the data subject(s).

Photographs will only meet the definition of personal data where they can be related to an identifiable individual. Where a photograph is stored with other information about the individual, such as in employment records, it will be personal

data. In such cases consent must be obtained from the data subject at the time of taking the image.

- employees consent is obtained on the Employee Details Form
- volunteers consent is obtained on the application form
- patients - patients are not routinely photographed. However it can be routine to photograph (for example), pressure ulcers, these are kept securely with the patient records. Where this happens consent must be obtained and recorded on the patient's medical record.
- All photographs of individuals taken by the Hospice for use in promotional, PR or Fundraising activities are treated as personal data and held by Fundraising and Communications team. The Fundraising and Communications team asks each individual to sign a consent form. Should the Hospice wish to use a photograph or send it to the media, the department notifies the individual in advance providing a proof of the photograph(s), the reason for its use and asks for written consent for publication

Communications holds its photographs and related consent forms on both physical and digital databases. Photographs of children require explicit consent from a parent or guardian.

Communications also holds "case study" stories of individuals – patients, carers volunteers etc – for its awareness raising purposes. These stories are held and employed under the same guiding parameters as the photographs above.

2. Good practice principles:

- do not use information that identifies individuals unless it is absolutely necessary
- keep the use of such information to a minimum and only use for the stated purpose
- be able to justify why you are using such information
- access to person-identifiable information should be on a strict 'need-to-know' basis
- ensure when you are sending confidential information by whatever means (internal post, external post, e-mail, fax telephone etc) that it is addressed and sent to a person who is entitled to receive it. You must take care to ensure it cannot fall into anyone else's hands, e.g. by telephoning first.

- ensure envelopes containing confidential information are sealed to prevent unauthorised access and clearly marked 'Personal and Confidential to be opened by addressee only'
- do not leave confidential files and correspondence where they can be read by unauthorised people
- password protect confidential files and keep passwords secure - change regularly, no sharing
- use a password protected screensaver on any computer holding confidential information or switch it off when unattended
- prevent virus attacks by taking care when opening e-mails and attachments or visiting new websites
- work on a 'clear desk' basis, securely storing hard copy personal information when it is not being used
- accompany visitors in areas normally restricted to employees and volunteers
- position computer screens away from windows to prevent accidental disclosures of personal information.

3. Destruction of Records

3.1 Private or confidential obsolete records must be permanently destroyed using one of the following:

- shredding.
- physical destruction of hard disks
- use of approved data erasure software

Relevant external law, regulation, standards:

The Caldicott Guardian Manual (2010),

The Caldicott Principles 2012; Revised Caldicott Principles 2016.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018