G6 – General Data Protection Regulations

Summary	Outlining North Yorkshire Hospice Care's policy on how we use and store information.
Document reference, eg, G41	*Which type of Organisational Document? Delete those not relevant* G6 Policy
Applies to	All of North Yorkshire Hospice Care Staff and Volunteers
Author	Director Emily Dobson (Strategy and Development)
Additional NYHC staff who have contributed	Cora Purnell (Deputy Chief Executive) Sally Leishman (Systems Manager)
Scrutiny group(s) who have seen this document	BOT
Ratified by	BOT
Date of ratification	02/02/2022
Equality Impact Assessment	
Data Protection Impact Assessment	
Version	
Available on	T Drive Website Relias
Related organisational documents	
Date of implementation	February 2022
Date of next formal review	February 2024

Document Control

Date	Version	Action	Amendments

1 Introduction

1.1 Policy scope

This policy covers all work and services carried out by North Yorkshire Hospice Care, a registered charity in England and Wales (518905). All staff and volunteers (where appropriate) operating its family of services, including Herriot Hospice Homecare, Just 'B', Saint Michael's Hospice and Talking Spaces, must therefore comply with the contents below. Throughout this document North Yorkshire Hospice Care and its family of services are referred to as 'we' 'us' 'our' for clarity and consistency.

1.2 Purpose of Organisation

The purpose of our services is wide ranging, from end of life services to bereavement support and counselling.

2. Policy Overview

To be able to provide the support to patients, employ staff, fundraise and carry out the finance functions our organisation holds a wide variety of information about individuals. Since it relates to identifiable individuals all of the activities using this data fall under the General Data Protection Regulations (GDPR). Our organisation have processes, documentation and records which are designed to ensure that we comply with the regulations and the organisation remains registered with the Office of the Information Commissioner, and we have put in place the procedures set out in this policy and procedure in order to meet the requirements of the Act and accompanying employment practices code.

The overall responsibility for Data Protection is held by the Board of Trustees and the Finance and Audit Trustee Subgroup, but is delegated to the following roles:

Information Governance Lead, Caldicott Guardian, Senior Information Risk Officer, and Information Security Officer.

This policy will set out the policies, documents, processes and procedures that our organisation have in place to meet the principles of GDPR.

3. Procedures

The GDPR introduces a set of Data principles which must be met by each organisation:

- Data is processed lawfully fairly and in a transparent manner
- Data is only collected for specific explicit and legitimate purposes

- Personal data is only processed where it is adequate, relevant and limited to what is necessary for the purpose of processing
- The personal data is accurate, and the organisation takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is only kept for the period necessary for processing
- Appropriate measures are in place to make sure that personal data is secure, protected against unauthorised or unlawful processing

4. Privacy Notices

Privacy notices have been produced for each point of contact that an individual may have with the organisation whether a patient or client, applicant, member of staff or volunteer, or a supporter or donor. The notices will explain the reasons for processing individual data, how it is used, the legal basis for processing, if it will be transferred or shared, how it is stored, archived and how long it will be kept before being destroyed.

5. Record of processing Activities

A register of the data processing activities for each department will be maintained, identifying clearly the types of data processes, purpose. Legal basis for processing, any disclosure, and transfer outside the EEA, retention periods and security measures which are applied to the data.

This will be reviewed and maintained at regular intervals.

6. Individual rights

Individuals may have the following rights in relation to their personal data:

- To make a subject access request as explained in more detail below
- To require the rectification of any inaccurate data
- To stop the processing or require the erasure of any data:
    - no longer necessary for the purposes of processing
    - if the individual's interests override the organisations legitimate grounds for processing and if this is the basis on which it is processed.
    - If processing is unlawful
- To stop processing for a period if data is inaccurate or if there is a dispute concerning the individuals rights overriding the rights of the organisation to legitimately process

Any subject data access requests for employee, volunteer or supporter information must be sent to the Information Governance Lead who will co-ordinate the process with the relevant team.

Any individual wishing take any of the steps other than making a subject access request should in the first instance contact the team responsible for the processing of their data who will then liaise with other teams as necessary.

In addition to providing a copy of the data undergoing processing our organisation will also confirm:

- If their personal data is being processed, the categories and source of the data if not from the individual
- To whom it may be disclosed, and safeguards to this process
- How long it is stored

- Rights in relation to correction or erasure of data, to restrict or object to processing
- Complaints process should the organisation have failed to comply with rights
- If any automated decision making takes place.

The data given will be provided in an electronic format in most cases unless specifically agreed otherwise and identity checks will be conducted with the individual before providing the data. If it is a large amount of data, we have the right to extend the response time from one month from the date of request to three but will inform the individual.

Should be request be manifestly unfounded or excessive, we are not required to comply and may choose to request a fee and will inform the individual of this decision.

Where the data subject access request relates to a deceased patient, the policies of the Department of Health and GMC will be followed in deciding the eligibility of the person making the application and the information to be disclosed. In all cases involving patient information the Medical Director as Caldicott Guardian will be consulted and involved in the provision of the information.

7. Data Security

We take the confidentiality and security of data seriously and have policies relating to Confidentiality and Information Security in place along with supporting procedures and technical measures. For full information please refer to those policies

Technical measures have been put in place to control access to the local area networks and to individual record systems, along with physical measures for hard copy files.

Individual employees are also responsible for protecting their passwords and maintaining the confidentiality and security of records and data they are processing as part of their role

8. Data Accuracy

To comply with the requirements of the GDPR it is important that all information is kept up to date. For each of the various IT and paper systems in operation the Director or Head of a department will be responsible for ensuring that there are processes in place for the maintenance of data and that housekeeping processes take place at regular intervals.

This includes archiving of records which are no longer current, and disposal or deletion of records in according with the requirements of the GDPR and as set out in the Records Management and Lifecycle policy.

9. Special category data

Information such as racial or ethnic origin, health conditions or criminal records are classed as special category data and will be processed in accordance with the GDPR requirements for such data,

10. Individual responsibilities

Individuals are responsible for helping us to maintain the accuracy of their personal data by informing the organisation of any changes to the data they have supplied.

Employees, volunteers, students or agency staff who process or have access to personal data as part of their role are required to adhere to the procedures in place to meet the requirements of GDPR and:

- To access only data they have the authority to access and only for the authorised purposes
- Not to disclose the data unless to individuals who are authorised
- Keep the data secure by protecting passwords, hard copy files, not using memory sticks or laptops to store personal data and following the information security policy.

- Not to remove any personal data either hard copy or in an electronic storage device from our premises without adopting appropriate security measures
- Not to store personal data on any private devices.

Failing follow these procedures or requirements may result in disciplinary action, termination of volunteering or placement as appropriate.

11. Training

We will provide appropriate training to everyone processing personal data during their induction and at appropriate intervals. The training will relate to the role and the types and volume of data accessed or processed.

12. The employment practices code

In addition to complying with the GDPR, we will continue to follow the Employment Practices issued by the ICO, and has incorporated them into the policies and procedures relating to recruitment and selection, employment records, monitoring at work and employment health record.

13. Monitoring at work

As part of the security systems operating at Crimple House a close circuit television system is in place which covers the external car park areas, entrances and ground floor corridors. The system operates 24 hours per day with images being recorded and stored electronically for up to 6 months.

This data will only be used to maintain the security of patients and staff working in the building or in the event of an incident of suspected misconduct.

In such circumstances the images will be used as part of the investigation and may be used as evidence. The images will not be used without notification for any other purpose.

CCTV is also used in some retail premises for the purposes of security and the avoidance of theft or settling of any disputes only. we will ensure that signs are visible to indicate the use of CCTV where it is installed.

The same applies to the monitoring of email, internet usage and telephone system where monitoring will be used to investigate where misconduct is suspected. The expectations of the organisation concerning the use of email or internet are set out in the relevant policies available as part of the organisational policies.

14. Loss of Data

The loss of any personally identifiable data will be reported and investigated following the procedures set out in the policy Reporting and investigating non-clinical incidents and near misses.