Nottinghamshire Hospice
adding life to days

POLICY/PROCEDURE INFORMATION (Policy no OP006)	
Subject	Data Retention Policy *(This policy is subject to periodic review and will be amended according to service development needs)*
Applicable to	All employees and volunteers who record/process personal data on behalf of Nottinghamshire Hospice
Date issued	March 2019
Next review date	March 2022
Lead responsible for Policy	Chief Executive Officer
Policy written by	Director of Finance and Resources
Notified to (when)	Chief Executive Officer
Authorised by (when)	Board of Trustees – 26 March 2019
CQC Standard if applicable	
Links to other Policies	Data Protection Policy and Procedures HR00005
Summary	The primary aim of this policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR. In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.
This policy replaces	

VERSION CONTROL		
Status	**Date**	**Reviewed date**
Original policy written by Maria Holmes, Director of Finance and Resources / SIRO for the organisation	Dec 2018	
Policy notified to Chief Executive Officer – Rowena Naylor-Morrell	Feb 2019	
Policy authorised by Board of Trustees	Mar 2019	Mar 2022
Updated control sheet and published on Policy Doc App	Mar 2019	
Updated logo and published on website	December 2020	
Reviewed and amendment made by Maria Holmes, Director of Finance and Resources. Updated on website	July 2021	

INDEX

APPENDICES		
Appendix	**Appendix Title**	**Page**
1	Data categories and retention periods	9

1. Introduction

This Policy sets out the obligations of Nottinghamshire Hospice Ltd, a company registered in Great Britain under number 509759, whose registered office is at 384 Woodborough Road, Nottingham, NG3 4JF ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child

This Policy sets out the type(s) of personal data held by the Company for legitimate business purposes, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Scope

2.1 This Policy applies to all personal data held by Nottinghamshire Hospice and by third-party data processors processing personal data on the Company's behalf.

2.2 Personal data, as held by Nottinghamshire Hospice is stored in the following ways and in the following locations:

a) The Company's servers, located at 384 Woodborough Road, Nottingham, NG3 4JF;

b) Electronically via computers, laptops and other mobile devices provided by the Company to its employees; located at 384 Woodborough Road, Nottingham, NG3 4JF, our Warehouse and all retail shops

c) Physical records stored at Nottinghamshire Hospice's offices, Warehouse and retail shops

d) Physical archived records stored by RADS; located at Colwick Business Park.

2.3 The Hospice utilizes SystmOne through CityCare for patient data however we are the data controller. A contract is in place regarding data processing. All data processed within SystmOne CityCare Community Palliative Care Unit by Nottinghamshire Hospice is retained by Nottinghamshire CityCare Partnership utilising their infrastructure and managed in accordance with their data retention policy and the NHS Records Management: Code of Practice. Nottinghamshire Hospice remains the data controller of the patient data with just the storage and maintenance being outsourced to Nottinghamshire CityCare Partnership as data processor.

3. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

3.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

3.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling , as set out in the Company's Data Protection Policy.

4. Technical and Organisational Data Security Measures

4.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All emails containing personal data must be password protected;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

f) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a 'signed for' delivery or courier service; and should be marked "confidential";

g) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested

h) All electronic copies of data stored on physical media should be stored securely and password protected;

i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;

j) Personal data must be handled with care at all times and should not be left unattended or on view;

k) Computers used to view personal data must always be locked before being left unattended;

l) No personal data should be stored on any work mobile device, without the formal written approval of the Senior Risk Information Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

m) Personal data may only be transferred to devices personally belonging to employees, agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;

n) All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be password protected;

o) All passwords used to protect personal data should be changed regularly and must be secure;

p) Passwords should not be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT support staff do not have access to passwords;

q) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

r) No software may be installed on any Company-owned computer or device without approval;

s) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Fundraising Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

4.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's

responsibilities under the GDPR and under the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

4.3 A Data Protection Impact Assessment (DPIA) is required under the GDPR any time a new project is started that is likely to involve "a high risk" to other people's personal information. The DPIA template should be completed when scoping the project.

5. Data Disposal

Upon the expiry of the data retention periods set out below in appendix 1 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

5.1 All Personal data stored electronically (including any and all backups thereof) shall be deleted

5.2 All Personal data stored in hardcopy form shall be shredded and recycled

6. Data Retention

6.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

6.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out below.

6.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Company's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

6.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

6.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

6.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

7. Roles and Responsibilities

7.1 The company's Senior Risk Information Officer shall be responsible for overseeing the implementation of this policy and for monitoring compliance with this policy, as well as the Company's Data Protection Policy and Procedures, in line with applicable data protection legislation.

7.2 The Senior Risk Information Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company**.**

7.3 Any questions regarding this policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Senior Risk Information Officer.

8. Implementation of Policy

No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after the date of publishing as stated on the front cover.

APPENDIX 1

Data Category	Type of Data	Retention Trigger	Retain For	Action	Retention Source
Regulatory	Audit Reports	Case closed	6 years	Review	Business Need
Regulatory	Breach Report	Case closed	2 years	Destroy	Business Need
Internal Regulatory Activities	Information created in relation to new policies, guidelines and research	Last Action	6 years	Review	Business Need
Stakeholder Engagement	Engagement with significant stakeholders	Last Action	6 years	Review	Business Need
Corporate Governance	Unsuccessful Trustee Recruitment Information	Creation	6 months	Destroy	Business Need
Corporate Governance	Trustee contact details, skills/application forms, election and term information	Resignation	7 years	Destroy	Business Need
Corporate Governance	Ambassadors contact details	Resignation	3 years	Destroy	Business Need
Corporate Governance	Memorandum of Understanding	End of Understanding	6 years	Destroy	Business Need
Corporate Governance	Committees and group minutes	Minutes agreed	6 years	Review	Business Need
Corporate Governance	Organisation wide corporate plans, policies, business continuity, risk management and strategies	Superseded	3 years	Review	Business Need
Corporate Governance	Corporate roles and responsibilities	Superseded	6 years	Review	Business Need
Corporate Governance	Non-clinical Complaints	Closure	1 year	Destroy	Business Need
Corporate Governance	Non-clinical Incidents and Accidents	Closure	7 years	Destroy	Business Need
Corporate Functions	Health and Safety Inspections, Property Management and Asset records	Last Action	6 years	Review	The National Archives Retention Scheduling: Departmental Accounts,

					H&S at work Act 1974 and supporting regulations, Limitation Act 1980
Corporate Functions	Documents relating to IT systems integral to their running and long term use	End of system life	3 years	Review	Business Need
Corporate Functions	Records and Information Management	Last Action	3 years	Review	Business Need
Corporate Functions	It Infrastructure	Last Action	3 years	Review	Business Need
Corporate Functions	Information Security	Last Action	6 years	Review	Business Need
Corporate Functions	Information Requests	Case Closed	2 years	Destroy	Business Need
Corporate Functions	Projects and Corporate Programmes	Last Action	3 years	Review	Business Need
Corporate Functions	CCTV	Last Action	1 month	Destroy	ICO CCTV Policy
Corporate Functions	Reception sign in book	End of Year	2 years	Destroy	Business Need
Finance	Financial Information	End of Financial Year	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Finance	Payroll Capita Reports	End of Financial Year	7 years	Destroy	HM Treasury guidelines, National audit office, Companies Act 2006
Finance	Employee contact, bank, tax and pension details	End of Employment	7 years	Destroy	Business Need
Human Resources	Employee files and Personal Development Records	End of Employment	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Human Resources	Disciplinary and Grievance, Examination and Testing, Accident and Ill Health	Last Action	7 years	Destroy	Limitation Act 1980
Human Resources	Job Descriptions and T&Cs	Last Action	7 years	Destroy	Limitation Act 1980

Human Resources	Training Material	Superseded	7 years	Destroy	Limitation Act 1980
Human Resources	Political Declarations	Superseded or end of employment	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Human Resources	Industrial Relations	Last Action	7 years	Destroy	Limitation Act 1980
Human Resources	Payroll sheets	End of Financial Year	7 years	Destroy	HM Treasury guidelines, National audit office, Companies Act 2006
Human Resources	Maternity, Paternity, Adoption and Sick Leave	End of Financial Year after return	7 years	Destroy	Statutory Sick Pay Regulations 1982, Statutory Maternity pay Regulations 1986, Statutory Paternity pay and Adoption pay Regulations 2002
Human Resources	Successful Recruitment Candidate Information	End of employment	7 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records and CIPD
Human Resources	Unsuccessful Recruitment Candidate Information	Last Action	6 months	Destroy	Limitation Act 1980
Human Resources	Staff pension, pay history and termination reasons	From DOB	100 years	Destroy	The National Archives Retention Scheduling: Employee Personal Records
Human Resources	Health Surveillance	Last Action	40 years	Destroy	Health and Safety at Work Act
Human Resources	Third Party emergency contact details provided by the staff member	End of Employment	Immediate	Destroy	Business Need
Human Resources	DBS Certificates	Creation	6 months	Retain top part of certificate only	Business Need
Human Resources	Medical Referrals	End of Employment	7 years	Destroy	Business Need
Legal	Policy Legal and Legal Advice	Last Action	6 year	Review	Limitation Act 1980

APPENDIX 1

Legal	Contracts	End of Contract	6 years	Review	The National Archives Retention Scheduling: Contractual Records
Legal	Unsuccessful Tenders	Last Action	400 Days	Review	The National Archives Retention Scheduling: Contractual Records
Legal	Building Contracts and Leases	End of Contract	12 years	Review	Limitation Act 1980
Volunteering	Unsuccessful Volunteer Recruitment Information	Creation	6 months	Destroy	Business Need
Volunteering	Successful Volunteer Recruitment Information	End of volunteering	3 years	Destroy	Business Need
Volunteering	DBS Certificates	Creation	6 months	Retain top part of certificate only	Business Need
Volunteering	Volunteer files, contact details and development records	End of volunteering	3 years	Destroy	Business Need
Retail	Customer contact and addresses, payment history /purchase history for refunds or voids	Transaction	3 years	Destroy	Business Need
Retail	Donor contact details for furniture collections	Once Collected	Instant	Destroy	Business Need
Retail	Gift Aid donor contact information	Sign up	7 years	Destroy	Business Need
Fundraising	Donor contact details	Last Action	3 years	Destroy	Business Need
Fundraising	Donor Bank details on leaflets and envelopes	Last Action	Instant	Destroy	Business Need
Marketing and Comms	Event and Challenge attendees contact details	Last Action	3 years	Destroy	Business Need
Marketing and Comms	E-newsletter subscribers via mailchimp	Until user unsubscribes	Instant	Destroy	Business Need

APPENDIX 1

Corporate Communications and Marketing	Market research reports, press releases, campaigns and projects, informer and image banks	Last Action	6 years	Review	Business Need
Corporate Communications and Marketing	Staff Events and Briefings, Public Engagement and Political Monitoring	Last Action	3 years	Review	Business Need
Corporate Communications and Marketing	Requests for Publications	Creation	4 weeks	Destroy	Business Need
Bereavement and Carer Support	Client files, contact details and personal information	Death/Discharge	7 years	Destroy	Business Need
Clinical	Patient files, contact details and personal information	Death/Discharge	10 years	Destroy	Business Need
Clinical	Clinical Incidents and Accidents	Closure	10 year	Destroy	Business Need
Clinical	Clinical Complaints	Closure	10 years	Destroy	Business Need
Communication Activities	Staff Mailboxes and Outlook	End of Employment	2 years	Delete	Business Need
Communication Activities	Physical Correspondents	Once Scanned	6 months	Destroy	Business Need
Organisation Wide	Internal Audits	Creation	3 years	Destroy	Business Need
Organisation Wide	Templates, Procedures, Team Information and Team Meetings	Last Action	3 years	Review	Business Need
Organisation Wide	Department Logs and Registers	Last Action	12 months	Review	Business Need
Organisation Wide	Team Administration	Creation	3 years	Review	Business Need
Organisation Wide	Management Information	End of Financial Year	6 years	Review	Business Need
Organisation Wide	Mobile device information for visitor Wi-Fi use	Creation	90 day	Destroy	Business Need

APPENDIX 1