Privacy Policy

Policy Owner:	**Director of Community & Business Development**
Policy Author:	**Director of Community & Business Development**
Classification:	**Corporate**
Policy No:	**020**
Date of Issues:	**December 2020**
Date of Review	**December 2023**
Total Number of Pages	**18**

INDEX

Introduction

This policy details how The Myton Hospices (Myton) use personal data which is collected from individuals for the purposes of patient care, fundraising, volunteering, marketing and information which is shared with Myton by third parties.

The policy also details how information provided to Myton might be used by third parties – for example when interacting with Myton social media accounts. A version of this policy is provided on our website as a privacy notice detailing how this applies to the individual – this is centred mainly on the collection and use of identifiable data collected via the website.

There are key differences in how we collect different types of information and in the legal basis for being able to use this information.

Scope

This policy applies to all aspects of personal identifiable data collected and recorded by Myton, including but not limited to:

- Patients and service users
- Donors and Supporters
- Human Resources (staff and volunteers)
- Finance and Facilities (contractors and suppliers)
- Organisational administrative information

Roles/Responsibilities

Management Board
It is the role of the Management Board and the Senior Leadership Team to define the Myton policy in relation to Privacy, taking into account legal and other requirements.

Chief Executive Officer
The Chief Executive is the officer accountable for compliance with the Data Protection Act 2018 and therefore with respect to an individual's right to privacy

Senior Information Risk Owner (SIRO)
The SIRO is a member of the Senior Leadership Team (the Director of Community & Business Development) who takes overall ownership of the Privacy Policy.

Information Governance Committee
It is the role of the Information Governance Committee to provide leadership in Myton for information governance ensuring compliance with statutory responsibilities, the requirements of administrative law including the Data Protection Act 2018 and the common law duty of confidentiality.

Caldicott Guardian
The Caldicott Guardian (at Myton this is the Medical Director) has the overall

responsibility of ensuring that requests for disclosure of any patient related information are appropriate and in accordance with the relevant data protection regulations. They should be involved in any proposed disclosure of confidential patient information or when disclosure of information, or issues of confidentiality give cause for concern.

Data Protection Officer
The Data Protection Officer (Head of IT) is the nominated officer on the Data Protection Register and is responsible for implementing the organisation's Data Security and Protection Policy. The Data Protection Officer is also responsible for processing and responding to all requests for information by data subjects and ensuring that Myton's data remains current and relevant, is stored safely and securely, and is destroyed appropriately when necessary**.**

Line Managers
Line Managers at Myton are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance on a day to day basis.

Staff and Volunteers
All staff and volunteers, whether permanent or temporary are responsible for ensuring that they familiarise themselves with this policy and relevant appendices and guidance and that they understand and comply with the responsibilities set out in them. If any member of staff or volunteer is unsure about any aspect of the policy or guidance they must seek clarification from their line manager or a member of the Information Governance Committee/Steering Group.

Individual responsibilities
Individuals who have access to personal data are required:

- to access only personal data that they have authority to access and only for authorised purposes
- not disclose personal data except to individuals who have appropriate authorisation
- to keep personal data secure (eg by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- not to remove personal data, or devices containing or that can be used to access personal data, from the Employer's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are used for work purposes
- The Data Protection Officer must be notified if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable.

Failure to comply with this policy and associated procedures may lead to disciplinary proceedings being taken which could lead to dismissal for gross misconduct.

Related Legislation

- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 2018)
- Computer Misuse Act 1990
- Copyright, designs and patents Act 1988 (as amended by the copyright computer programmes regulations 1992)
- Crime and Disorder Act 1998
- Data Protection Act 2018
- Electronic Communications Act 2000
- Human Rights Act 1998
- Mental Capacity Act 2005
- Regulations of Investigatory Powers Act 2000 (RIPA)
- Health & Social Care (Quality & Safety) Act 2015
- General Data Protection Regulation 2018

Related Policies and Procedures

- Recruitment & Selection Policy
- Data Security & Protection Policy
- Consent Policy
- Information Governance Policy
- Safeguarding Vulnerable Adults at Risk Policy
- Safeguarding Children and Young People Policy
- Non-Clinical Records Management Policy
- Clinical Records Management Policy
- Complaints Policy
- Equality, Diversity & Inclusion Policy
- Internet, Email and Computer Usage Policy
- Data Quality Policy
- Accident & Incident Reporting Policy
- Income Generation Policy
- Ethical Fundraising Policy
- Social Media Policy

How information is collected in relation to individuals

Patient Information:
Information in relation to patients is collected from a range of sources. For example patient information will be provided when a hospital or GP refers a patient to us, referrals might also come from other individuals and organisations engaged in the provision of patient care such as Community Nurses and Care Homes. For some services individuals can also self-refer to us in order to access our services without being referred by another healthcare provider or organisation.

Sharing of relevant clinical information is important to ensure effective clinical handover for the purpose of providing safe and effective care to the patient and appropriate support for their family and as such there is a specific exemption for this purpose under data protection legislation.

Other Information provided directly

We may also obtain information about individuals when they take part in one of our events, make a donation, apply to volunteer for us, purchase products and services, donate goods to our retail outlets or sign up to our Lottery - this information is provided directly by the individual.

Other Information provided indirectly by individuals

Information may be shared with us by third parties which may include:

- Independent event organisers, for example **The London Marathon** or **Skyline Registrations** and fundraising/social media sites such as **Just Giving** or **Facebook**
- Professional subcontractors acting on our behalf who provide us with technical, payment or delivery services such as secure online payment processing

Individuals are advised to check the privacy policy applicable when they enter data on a third party website.

We strive to ensure that all individual's data is kept safe and secure, and only processed in accordance with current Data Protection legislation. Individuals are only communicated with in the way(s) that they have agreed to. Individuals can change their contact preferences/consent at any time by contacting the Donor & Supporter Care Team at DSC@mytonhospice.org or calling **01926 358 383.**

Information collected via our website:
Like many organisations we automatically collect the following information when individuals visit our website.

This can include technical information, such as the type of device being used, IP address, browser and operating system being used to connect a computer to the internet. This information may be used to improve the services we offer.

Information is also collected about visits to the website for example we collect information about pages visited and how the website is navigated, i.e. length of visits to certain pages, products and services viewed and searched for, referral sources (e.g. how the individual arrived at our website).

We collect information from the website by **using** cookies. Further information on cookies can be found under the '**Use of Cookies**' section on page 14 of this policy.

Social Media
When individuals interact with Myton Hospice on platforms such as **Facebook** and **Twitter** we may obtain information about them (for example, when they publicly tag us in an event photo). The information we receive will depend on the privacy preferences the individual has set on those types of platforms.

What type of information is collected?

Patient Information:

For individuals using our clinical services we will need to collect information such as the name, age, address, gender, and possibly sensitive personal information concerning health and wellbeing, ethnic origin, sexual orientation, and religion . In order to provide complete care we may also collect some information about family members and carers of the patient. For individuals who stay on or visit our premises, such as our Inpatient Unit, we may collect images of individuals on CCTV.

It may also be necessary to take still images of patients for medical purposes, such as in the case of pressure ulcers. Any such images are stored securely and only identifiable by the patient hospice number.

Any telephone calls made about patients may be recorded for training and quality purposes.

We may receive data about patients and their families and carers from other healthcare providers in line with the provisions of sharing of information being explicitly for the provision of patient care only, this might form part of the initial referral or is obtained from the individual directly as a result of them receiving care and services from us.

In using our website the personal information we collect, store and use might include:

- Name and contact details (including postal address, email address and telephone number)
- Date of birth
- Information about activity on our website and about the device used to access it, for instance your IP address and geographical location
- The reason someone has chosen to support Myton
- Bank or credit card details. If individuals make a donation online or make a purchase, although card information is not held by us, it is collected by our third party payment processors, who specialise in the secure online capture and processing of credit/debit card transactions.
- Information as to whether the individual is a UK taxpayer so we can claim gift aid; and any other personal information which is shared by the individual

Data protection laws recognise certain categories of personal information as sensitive and therefore requiring greater protection, for example information about health, ethnicity and religion.

We do not usually collect sensitive data about individuals unless there is a clear and valid reason for doing so for example in the event of a patient referral or in order to access our care services. Data protection laws allow us to, for example, ask for health information from individuals when they are taking part in one of our events.

How and why is individual's information used?

Patient Information

Information in relation to our clinical services is used strictly for the purposes of the provision of patient care or the provision of support services to other individuals including family and friends of the patient.

Information relating to patients is strictly held within Myton Hospices it is not sent elsewhere for processing purposes or shared with external organisations except where necessary for the care of the patient. For the benefit of the patient, we may need to share information from your health records with NHS and non-NHS organisations who are providing you with care or other services, such as social services or private healthcare organisations.

We may also be asked to share basic information about patients, such as their name and parts of their address, which does not include special category information from their health records. Generally, we would only do this to assist another organisation to carry out their statutory duties (such as usages of healthcare services, public health or national audits)

The only exemptions relating to the transfer of information other than for the purposes set out above, is that patient and non-clinical records are sent for archiving at Oasis Group, a secure storage provider, and subsequent destruction upon the expiry of the required retention period for these records.

Information about patients may also be used for analysis of our services and for monitoring of service quality. For data used outside of Myton hospices or for staff not directly engaged in the provision of patient care only aggregated data is used – this would for example include data relating to the number of individuals seen and overall service activity. Where there is no legal basis that permits us to use identifiable patient information we will always ensure that such data is anonymised to prevent the identification of individual patients and only share the minimum amount of data necessary.

Supporter Information

Information is used for:

- Providing individuals with the services, products or information they have asked for.
- Processing orders that individuals have submitted.
- Carrying out our obligations under any contracts entered into between the individual and Myton Hospices, including Lottery membership and the Retail Gift Aid scheme
- Keeping a record of an individual's relationship with us
- Conducting analysis and marketing research so we can understand how best to improve our services, products or information
- Checking for updated contact details against third party sources so we can stay in touch with individuals
- Seeking views, comments or opinions on the services we provide

- Notification of changes to our services
- Sending communications that individuals have requested and that may be of interest to them. For example information about campaigns, fundraising appeals, promotions of good and services or job applications

Communication

We may use individual's contact details to provide them with information about the vital work we do, our fundraising appeals and opportunities to support us, as well as the products and services available, if we think it may be of interest to the individual.

Email/Phone

We will only send marketing and fundraising communications by email and phone where the individual has explicitly provided prior consent. Individuals may opt out of our marketing communications at any time by clicking the unsubscribe link at the end of our marketing emails or emailing unsubscribe@mytonhospice.org with their details.

Post

We may send marketing and fundraising communications by post to those that have given us explicit consent to do so. For supporters who were first involved with Myton prior to 25 May 2018 (GDPR), we may send marketing and fundraising communications by post unless individuals have told us that they would prefer not to hear from us in this way. We may also use legitimate interest when contacting some supporters about products and services we feel may be of interest to them.

Consent & Communication Preferences

At Myton, we value our donors and supporters and recognise that without them, we would not be able to continue our work caring for terminally ill patients and their families across Coventry and Warwickshire.

We are committed to communicating with individuals in their preferred manner and putting you in control of your data.

We will not use personal information for marketing purposes if an individual has indicated that they do not wish to be contacted and will retain their details on a suppression list to help ensure that we do not continue to contact them. However, we may still need to contact them for administrative purposes for example where we are processing a donation or thanking individuals for their participation in an event.

How long is information kept for?

We will keep information for no longer than is necessary for the purposes it was collected for, the length of time we retain personal information for is determined by operational and legal considerations. For example, we legally are required to hold

some types of information to fulfil our statutory and regulatory obligations for example tax and accounting purposes.

Details of the retention period for data is set out in the following policies:

- Policy for the Retention and Disposal of Non-Clinical Records
- Clinical Records Management Policy

Who has access to personal information?

We do not sell or share personal information with third parties for marketing purposes, nor is patient information transferred to third parties except where we are required by law to disclose this information and for the purposes of continuing patient care with other health service providers and those engaged in the care of the patient.

We may disclose information to third parties in order to achieve the other purposes set out throughout this policy.

Third parties working on our behalf

We may pass information to our third party service providers, suppliers, agents, subcontractors and other associated organisations for the purposes of completing tasks and providing services on our behalf (for example to process donations, to send mailings or process our Lottery).

When we use these third parties, we disclose only the personal information that is necessary to deliver the services and we have a contract in place that requires them to keep personal information secure and prevents them from using it for their own direct marketing purposes.

We will not release personal information to third parties for them to use for their own direct marketing purposes, unless it has been agreed with the individual(s) concerned, or we are required to do so by law.

Lawful Processing

Data protection law requires us to rely on one or more lawful grounds to process personal information. We consider the following grounds to be relevant:

Patient Information

Patient information in relation to health is treated as special category data, the lawful basis for processing personal information in this instance is met under section 9 of the General Data Protection Regulations 9(2)(h). 'Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional'

Safeguarding

Some members of society are recognised as needing protection, for example children and vulnerable adults. If a person is identified as being at risk from harm we are expected as professionals to do what we can to protect them. In addition we are bound by certain specific laws that exist to protect individuals. This is called "Safeguarding".

Where there is a suspected or actual safeguarding issue we will share information that we hold with other relevant agencies whether or not the individual or their representative agrees. The purpose of the processing is to protect the vulnerable person.

The lawful basis for processing personal information in this instance is met under section 6 of the General Data Protection Regulations: 6(1)(c) '…necessary for compliance with a legal obligation…'Other Personal Information

Specific Consent

Where individuals have provided specific consent to us using their personal information in a certain way, such as to send email, text and/or telephone marketing. This would also include patient health information for the purpose of providing our services.

Performance of a contract

Where we are entering into a contract with individuals or performing our obligations under it for example with members of our Lottery.

Legal obligation

Where necessary so that we can comply with a legal or regulatory obligation to which we are subject, for example where we are ordered by a court or regulatory authority like the Charity Commission or Fundraising Regulator.

Vital interests

Where it is necessary to protect life or health (for example in the case of medical emergency suffered by an individual at one of our events) or a safeguarding issue which requires us to share information with the emergency services.

Legitimate interests

Where it is reasonably necessary to achieve our or others' legitimate interests (as long as what the information is used for is fair and does not duly impact on the rights of the individual).

We consider our legitimate interests to be running The Myton Hospices as a charitable organisation in pursuit of our aims and ideals. For example to:

- Send communications which we think will be of interest
- Conduct research to better understand who our supporters are to better target our fundraising
- Monitor who we deal with to protect the charity against fraud, money laundering and other risks
- Enhance, modify, personalise or otherwise improve our services /communications for the benefit of our supporters
- Understand better how people interact with our website

When we legitimately process personal information in this way, we consider and balance any potential impact (both positive and negative) on an individual, and their rights under data protection laws. We will not use individual's personal information where our interests are overridden by the impact on them, for example, where use would be excessively intrusive (unless, for instance, we are otherwise required or permitted to by law).

Profiling (non-patient related data)

We may analyse the personal information we collect to create a profile of someone's interests and preferences so that we can contact them in the most appropriate way and with the most relevant information. From time to time we carry out an analysis of our supporters and the donations they have made. Some of the results from this analysis provide us with an indication of the likely donations that we may receive in the future which allows us to plan accordingly. We may also enhance the data we hold on a supporter by receiving information about them from public sources.

Individual rights

Under UK data protection law, individuals have certain rights over the personal information that we hold about them. Here is a summary of the rights which apply:

Right of access

Individuals have a right to request access to the personal data that we hold about them. Individuals also have the right to request a copy of the information we hold about them, and we will provide them with this unless legal exceptions apply.

If individuals wish to access the information we hold about them, they need to send a description of the information they want to see and proof of identity by post to the address provided below. We will provide them with this information within the timescales set out by the Data Protection Act.

Right to have inaccurate personal information corrected

Individuals have the right to have inaccurate or incomplete information we hold about them corrected. The accuracy of personal information is important to us so we're working on ways to make it easier for them to review and correct the information that we hold about them. If an individual wants to update their personal information or is concerned that any of the information we hold is inaccurate or out

of date, they can contact us via email at **DSC@mytonhospice.org** or post (see below). Alternatively, they can telephone **01926 358383**.

Right to restrict use

Individuals have a right to ask us to restrict the processing of some or all of their personal information if there is a disagreement about its accuracy or we are not lawfully allowed to use it.

Right of erasure

Individuals may ask us to delete some or all of their personal information and in certain cases, and subject to certain exceptions; we will do so as far as we are required to. If necessary, we will anonymise that information, or make it inactive, rather than delete it.

Right for personal information to be portable

If we are processing personal information (1) based on individual consent, or in order to enter into or carry out a contract with them, and (2) the processing is being done by automated means, the individual may ask us to provide it to them or another service provider in a machine-readable format.

Right to object

Individuals have the right to object to processing where we are using their personal information (1) based on legitimate interests, (2) for direct marketing or (3) for statistical/research purposes.

If individuals wish to exercise any of the above rights, they should email us at **DPO@mytonhospice.org** or write to **Data Protection Officer, The Myton Hospices, Myton Lane, Warwick, CV34 6PX.**

We may be required to ask for further information and/or evidence of identity. We will endeavour to respond fully to all requests within the timescale set out within the Data Protection Act, however if we are unable to do so we will contact the requestor with reasons for the delay.

Please note that exceptions apply to a number of these rights, and not all rights will be applicable in all circumstances. For more details we recommend you consult the guidance published by the UK's Information Commissioner's Office, **https://ico.org.uk/**

Keeping personal information safe online when using our website

When individuals give us personal information, we take steps to ensure that appropriate technical and organisational controls are in place to protect it.

Any sensitive information (such as credit or debit card details) is encrypted and protected with the following software 128 Bit encryption on SSL. When they are accessing our website and are on a secure page, a lock icon will appear usually at the top of the page next to the website address (URL).

Non-sensitive details (such as email address etc.) are transmitted normally over the internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect personal information, we cannot guarantee the security of any information individuals transmit to us, and they do so at their own risk. Once we receive their information, we make our best effort to ensure its security on our systems. Where we have given (or where the individual has chosen) a password which enables them to access certain parts of our website, they are responsible for keeping this password confidential. We ask them not to share their password with anyone.

Use of 'cookies'

Our website uses cookies. A cookie is a small file of letters and numbers that we put on a computer. By using our website, an individual agrees we can set and use cookies. These cookies allow us to distinguish users of our website, for example being able to store a country preference when completing a form. This website does not store any information that would, on its own, allow us to identify individual users of this service without their permission. Other cookies that may be used by this website are used either solely on a per session basis or to maintain user preferences.

Links to other websites

Our website may contain links to other websites run by other organisations. This policy applies only to our website, so we encourage individuals to read the privacy statements on the other websites they visit. We cannot be responsible for the privacy policies and practices of other websites even if they access those using links from our website.

In addition, if an individual linked to our website from a third party site, we cannot be responsible for the privacy policies and practices of the owners and operators of that third party site and recommend that you check the privacy policy of that third party site.

16 or under

We are concerned to protect the privacy of children aged 16 or under. If individuals are aged 16 or under, they should get their parent/guardian's permission beforehand whenever they provide us with personal information.

Vulnerable circumstances

We are committed to protecting vulnerable supporters, customers and volunteers and appreciate that additional care may be needed when we use their personal information. In recognition of this, we observe good practice guidelines in our interactions with vulnerable people.

Transferring personal information outside of Europe

As part of the services offered through our website, the information which individuals provide to us may be transferred to countries outside the European Economic Area ("EEA"). They should be aware that these countries may not have similar data protection laws to the UK. By submitting their personal data, they are agreeing to this transfer, storing or processing. If we transfer their information outside of the EEA in this way, we will take steps to ensure that appropriate security measures are taken with the aim of ensuring that privacy rights continue to be protected as outlined in this policy by means of ensuring the company is using the Privacy Shield to protect their data.

If individuals use our services whilst they are outside the EEA, their information may be transferred outside the EEA in order to provide them with those services. We undertake regular reviews of who has access to information that we hold to ensure that personal information is only accessible by appropriately trained staff, volunteers and contractors.

Appendix 1

Useful third party website policies

Facebook **-** https://www.facebook.com/policy.php

Twitter - https://twitter.com/en/privacy

Sage - https://www.sage.com/en-gb/legal/privacy-and-cookies/

Rapidata - http://rapidataservices.com/terms-conditions/

Mailchimp - https://mailchimp.com/legal/privacy/

Linkedin - https://www.linkedin.com/legal/privacy-policy?trk=

Instagram - https://help.instagram.com/155833707900388

Hotjar - https://www.hotjar.com/legal/policies/privacy

Google analytics - https://policies.google.com/privacy?hl=en-GB&gl=uk

Document Control Sheet – Privacy Policy

Development and Consultation	2020 - Developed By: Director of Community & Business Development, Clinical Governance & Quality Lead, Data & Information Governance Manager, Head of IT, Digital Marketing & Social Media Executive, Individual Giving Manager, Executive PA, Medical Administration Team Leader, Information Governance and IT Committee
Dissemination	The policy will be distributed, by the Clinical Governance & Quality Lead to all relevant Department Manager/Line Managers for dissemination to staff. An electronic copy can be found in Team Room/Policies & Procedure/ Active Policies.
Implementation	Implementation date will be the date the policy is issued by the Clinical Governance & Quality Lead and supersedes all previous policy versions.
Audit	The policy has been developed in line with the Policy Development Process.
Review	The owner of the policy is responsible for reviewing and updating the policy every 3 years
Links with other documents that guide practice and any relevant Myton Policies	Information Governance Policy Data Quality Policy Data Security and Protection Policy Policy for the Retention and Disposal of Non-Clinical Records Clinical Records Management Policy

Essential Standards of Quality & Safety	This policy supports the Organisation in its compliance with the Care Quality Commission's Essential Standards of Quality and Safety in the following areas: **This policy supports the Organisation in its Related Polices and Documents** Information Governance Policy Data Quality Policy Data Security and Protection Policy Policy for the Retention and Disposal of Non-Clinical Records Clinical Records Management Policy
Regulation of the Health & Social Care Act 2008 (Regulated Activities) Regulations 2010 Regulation 17, 24,21	Outcome: 1,6,21