

Hospice Privacy Notice

Protecting Your Data

Introduction

This privacy notice explains in detail why we use your personal data which we, the Hospice (Data Controller), collects and processes about you. A Data Controller determines how the data will be processed and used and who this data will be shared with. We are legally responsible for ensuring that all personal data that we hold, and use is done so in a way that meets the data protection principles under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. This notice also explains how we handle that data and keep it safe.

The Hospice is a Data Controller. A Data Controller determines how the data will be processed and used within their organisation and with others they can share the data with.

We are legally responsible for ensuring that all personal data that we hold, and use, is done so in a way that meets Data Protection legislation, particularly the data protection principles under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. We need to make sure that where we process your personal data, we can do so legally. Article 6 of the UK GDPR lists 6 lawful bases for processing personal data, at least one must apply. This notice will explain the legal bases available, where we process personal data and in addition explains how we handle that data and keep it safe and secure.

The Hospice is committed to looking after your personal data and it is the responsibility of all staff throughout the organisation to make sure of this. Our staff are required to sign up to and abide by our Code of Confidentiality Policy.

The Hospice employs specific roles to provide leadership and direction to ensure accountability and transparency to support compliance with Data Protection law.

These roles include:

Caldicott Guardian

The Hospice has a Caldicott Guardian. A Caldicott Guardian is a senior person within a health or social care organisation, preferably a health professional, who makes sure that the personal information about those who use its services is used legally, ethically

and appropriately, and that confidentiality is maintained. The Caldicott Guardian for the Hospice is:

Louise Charnock
Queenscourt Hospice, Town Lane, Southport, PR8 5DY
Tel: 01704 517926
Email: hospice@queenscourt.org.uk

Senior Information Risk Owner (SIRO)

The SIRO is the Executive Director of Strategy & Business Development at the Hospice with overall responsibility for managing organisational information risk, security of information and putting strategies in place to control the identified risks. Our SIRO is Sam Hawksley.

Data Protection Officer (DPO)

Under the UK GDPR all public bodies must nominate a Data Protection Officer. The DPO is responsible for advising on compliance, training and awareness and is the main point of contact with the Information Commissioner's Office (ICO). The DPO for the Hospice is:

Our Data Protection Officer (DPO) is Camilla Bhondoo.

Our DPO can be contacted via the following means:

Address: Jubilee Court, Academy Site, Waterside, St Helens, WA9 1TT
Email: IG@midmerseyda.nhs.uk

We will continually review and update this privacy notice to reflect changes in our services and to comply with changes in the law. When such changes occur, we will revise the last updated date as documented in the version status in the header of this document.

What we do?

We are here to provide care and treatment to you as our patients. In order to do this, we will keep personal demographic data about you such as your name, address, date of birth, telephone numbers, email address, NHS Number etc and your health and care information. Information is needed so we can provide you with the best possible health and care. We also use your data to:

- Confirm your identity to provide these services and those of your family / carers

- Understand your needs to provide the services that you request
- Obtain your opinion on our services (with consent)
- Prevent and detect fraud and corruption in the use of public funds
- Make sure we meet our statutory obligations, including those related to diversity and equalities
- Adhere to a legal requirement that will allow us to use or provide information (e.g. a formal Court Order or legislation, investigations)

Definition of Data Types

We use the following types of information / data:

Personal Data

This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under UK GDPR, this now includes location data and online identifiers.

Special categories of data (previously known as sensitive data)

This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under UK GDPR, this now includes biometric data and genetic data.

Personal Confidential Data (PCD)

This term came from the [Caldicott review](#) undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Pseudonymised Data or Coded Data

Individual-level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity. When data has been

pseudonymised it still retains a level of detail in the replaced data by use of a key / code or pseudonym that should allow tracking back of the data to its original state.

Anonymised Data

This is data about individuals but with all identifying details removed. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Aggregated Data

This is statistical information about multiple individuals that has been combined to show general trends or values without identifying individuals within the data.

Why we collect personal data about you?

As an organisation providing healthcare the Hospice has a legal justification to collect and use information about our service users for direct healthcare purposes.

It is important that our staff know as much about your physical health as possible so that we can give you appropriate care and attention. Our aim is not to be intrusive, and we won't ask irrelevant or unnecessary questions. We ask you for information so that we can keep your details accurate, relevant and up to date, and to give you the best treatment available.

This personal data can be held in a variety of formats, including paper records, electronically on computer systems, in video and audio files.

If your details change you should let a member of your healthcare team know as soon as possible. The Hospice encourages you to be the 'guardian' of your own safety by providing this information.

We collect your information from you, your family members, close friends and carers who attend our services, for example you may be listed as Next of Kin or an Emergency Contact. We keep records about you and our contact with you electronically.

Your information is used for:

- Direct care to ensure you get the best possible care and treatment
- To invite and provide you to use our family, friends and carer support services
- To ensure that we have a record of our sessions for your continued support

What we will collect?

Depending on what you are being treated for the personal data we collect from you will differ, here are some examples:

- Basic details such as name, address, date of birth, next of kin and contact details including phone number and email address, where applicable. .
- Details of your family, relatives and carers
- Details about you such as racial or ethnic origin, gender, occupation, lifestyle and social circumstances, religion or similar belief
- Current health problems and any contacts that we have had with you, old and new
- Visual images, personal appearance and behaviour
- Notes and reports about your health, treatment and care and results of investigations and tests
- Any relevant information from other health and social care professionals, who are, or have been, involved in your care including General practices (GPs), Acute hospitals, Ambulance services, Clinical Commissioning Groups, Community, Nursing Homes, and many others including family and carers

Information about you may also be needed for the following reasons:

- To ensure that our services meet your needs
- To assist staff to review the care that they provide and to ensure that it is of the highest standard
- To investigate complaints or legal claims
- To ensure that the Hospice receives funding from its commissioners to pay for your care
- To prepare statistics on our performance in order to manage, improve and extend the services we are able to provide to you
- To prevent or detect fraud and corruption in the use of public funds
- In some cases, phone calls may be recorded for training and information purposes
- When information is used for statistical or financial purposes, strict measures are taken to ensure that you cannot be identified from your information. You have the right to withhold information unless the law requires us to obtain it

What is our legal basis for processing your personal data?

Under the UK GDPR we cannot process / use your personal data without a legal basis. We must identify the appropriate legal basis depending on how we are using your data.

The UK GDPR details 6 legal bases (Article 6) for processing personal data:

- A - Consent
- B - Contract
- C - Legal obligation
- D - Vital interests
- E - Public task
- F - Legitimate interests

Where special category data is processed, we must also apply a legal condition from Article 9, special category data in the Hospice case is Health data:

- A - Explicit consent
- B - Employment, social security and social protection (if authorised by law)
- C - Vital interests
- D - Not-for-profit bodies
- E - Made public by the data subject
- F - Legal claims or judicial acts
- G - Reasons of substantial public interest (with a basis in law)
- H - Health or social care (with a basis in law)
- I - Public health (with a basis in law)
- J - Archiving, research and statistics (with a basis in law)

For the majority of our processing, we require your personal data for direct patient care, this means we apply the following legal basis (i.e. consent is not required):

Article 6 (e) and Article 9 (h)

We do not need a legal basis where we have anonymised your personal data.

More information on legal bases can be found here on the [ICO's website](#)

Who we share your personal data with?

We sometimes need to share the personal data we process with yourself as a service user with other organisations. We will only do if we have a legal basis to do so. What follows is a description of the types of organisations we may need to share some of the personal data we process with for one or more reasons. In the following situations we will not need to ask your permission (gain consent) and can use another legal basis to share the data that is required:

- Staff;
- healthcare, social and welfare organisations;
- suppliers, service providers, legal representatives;
- auditors and audit bodies;
- educators and examining bodies;
- survey and research organisations;
- professional advisers and consultants;
- business associates;
- police forces;
- security organisations;
- central and local government;
- voluntary and charitable organisations.

Any organisation that receives your personal data from the Hospice is also bound by a legal duty of confidentiality under the UK GDPR. An information sharing agreement is often in place with those organisations to ensure that it is kept confidential and secure but what is key is making sure we establish the right legal basis before we share your data.

Occasionally there are exceptional circumstances that mean we may have to share your information, such as when you or someone else is at significant risk of harm, or where the law requires such information to be disclosed, e.g. for the prevention or detection of a crime.

When we share your personal data with relatives, partners, carers and friends

Relatives, partners, carers and friends will be kept up to date about the progress of your treatment only if you have agreed to this and a record has been made of this agreement. If you change your mind this agreement can be withdrawn, and your new decision will be recorded.

If an individual lacks capacity to consent to the collection or sharing of their information or making a request for access to their health record, then a decision may be made either by a health/social care professional or someone else appointed to act on their behalf.

Information may also be shared when a legal order is in place e.g. Power of Attorney, Guardianship or Court Orders.

Other areas where we may process your personal data

Artificial Intelligence (AI)

Artificial Intelligence (AI) is expanding, and we are pleased to support this 'new' area of technology which is here to support our clinicians and provide intelligent care. The use of AI is expanding across the Healthcare. Before any AI implementation the Hospice must ensure that they have looked and assessed both the privacy and security risks. Only AI that has provided the Hospice with significant assurance will be utilised, following a vigorous approval process. We look to roll out AI in areas that require support however we will ensure that there is always clinical human oversight.

How long do we keep your personal data for (Records Retention and Destruction)?

Whenever we collect or process your data, we will only keep it for as long as is necessary for the purpose it was collected. In the NHS, all providers and commissioners apply retention schedules in accordance with the Records Management Code of Practice (refer to Link section below). This code is based on current legal requirements and professional best practice and sets the required standard of practice in the management of records for those who work within or contract to NHS organisations in England.

For healthcare purposes, records, these records need to be kept for long periods of time and remain available to access. Consequently, it is unlikely that a record or information contained in the record will be erased or deleted if such a request is made.

Following the retention period, the record will be fully reviewed and confidentially destroyed if it is deemed appropriate.

Destruction

Destruction of data will only happen following a "review" of the information at the end of its retention period. Where data has been identified for disposal we have the following responsibilities:

- To ensure that information held in manual form (regardless of whether originally or printed from the IT systems) is destroyed using a cross cut shredder or subcontracted to a reputable confidential waste company (as identified in the table below) that complies with European Standard EN15713.
- To ensure that electronic storage media used to hold or process information are destroyed or overwritten to current national cyber security standards.
- To ensure that any arrangement made to sub-contract secure disposal services from another provider, complies with the NHS Standard Contract and with assurance that the sub-contractor's organisational and technical security measures comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

How we keep your personal data confidential and secure?

We are committed to protecting your privacy and will only process personal data in accordance with the UK GDPR, the Data Protection Act 2018, the Common Law Duty of Confidentiality and the Human Rights Act 1998. We do this by using secure technologies and following safe practices.

All information is subject to rigorous measures and procedures to make sure it cannot be seen, accessed or disclosed to any inappropriate persons. We have an Information Governance Framework detailed within our Information Governance Strategy that explains the information governance / data security within the Hospice.

Access to electronic data is password protected on secure network and / or online systems and, where it is practically possible, paper documentation is filed securely in lockable storage cabinets. Where documentation is required to be transported between sites measures are in place to ensure their safe delivery.

Technical assurance is provided regarding IT / Cyber processes in place as the Hospice are required to complete the Data Security and Protection Toolkit (DSPT) which is an online assessment that must be completed every year by organisations who process Personal Data. It looks at what data protection, IT security and cyber security measures are in place. The Hospice IT Department regularly monitor the network for potential vulnerabilities and attacks and look to always ensure security is strengthened.

Where we engage the services of Data Processors / suppliers, the Hospice is required to carry out a 'due diligence' on the organisation. This means that the organisation looking to process your data on our behalf is subject to interrogation, looking specifically at what data protection and IT security they have in place to ensure they are safeguarding your data, this is documented via a Due Diligence Questionnaire and a Data Protection Impact Assessment and reviewed by our IT Security Team, IG Team, DPO and final approval is provided by the Hospice SIRO.

Our IT Services provider (Mid Mersey Digital Alliance), regularly monitor our systems for potential vulnerabilities and attacks and look to always ensure security is strengthened.

Everyone working for the NHS has a legal duty to keep information about you confidential and comply with the [common law duty of confidentiality and other NHS guidance](#).

All of our staff, including contractors, receive appropriate and ongoing information governance / data security training to ensure they are aware of their personal responsibilities and have contractual obligations to uphold confidentiality, enforceable through disciplinary procedures.

We have incident reporting and management processes in place for reporting any personal data breaches or incidents. We learn from such events to help prevent further issues and inform data subjects like yourselves of breaches when required.

In line with Data Protection legislation the Hospice has assigned roles are required to ensure the Hospice embed and embrace the Information Governance Framework, please refer to the Introduction section for more information.

Purposes other than direct care (secondary use)

Secondary use of data in the NHS is when patient data is not used for direct care but for other secondary purposes such as commissioning, risk stratification, financial and national clinical audit, healthcare management and planning, research and public health surveillance.

Disclosure of anonymised, pseudonymised or aggregated data (see section 'Definitions' for more information) will often satisfy a number of secondary uses and must be used in preference to patient / personal data. Consent for disclosure of effectively de-identified data is not required as it is not personal data. De-identification / pseudonymisation processes must occur before data leaves the source organisation. If a request is for identifiable data and the source organisation feels that de-identified data would suffice clarification should be obtained as to why identifiable data is required other than, exceptionally, where mandated by law such as under a Section 251 approval as per the NHS Act 2006 (see section below) or patient consent is obtained. Where consent is being relied upon you have the right to dissent from the disclosure of your personal data for secondary purposes unless the law compels disclosure.

Section 251 of the NHS Act 2006

Section 251 of the NHS Act 2006 provides a mechanism which can enable the use of confidential information for certain purposes where it is unreasonable for consent to be obtained or that would otherwise be unlawful (e.g. information from NHS Digital on commissioning, Risk Stratification and Invoice Validation) through an application made to the Confidentiality Advisory Group (CAG).

The use of data for which an application is made must be for a medical purpose as defined in section 251 (12) of the NHS Act 2006. This includes medical research and management of health and social care services.

Further information can be found on the Health Research Authority website

Research and Planning - Why we do research

Research in the NHS helps to improve public health and patient care, it's how we improve treatments and pathways in the NHS and make a real difference to people's lives.

Our research links closely with secondary care, mental health and community healthcare to ensure patients and their wellbeing are at the heart of everything we do. It covers all types of studies ranging from early-stage developments of new treatments to large scale population-wide studies. It means patients have access to some of the most cutting-edge treatments

The use of your personal data for research

Some research will require your direct involvement (especially if taking part in clinical trials) in which case the circumstances will be fully explained to you and your express consent will be required. If you do not consent, then you will not be included in the research and/trial.

Sometimes, researchers need access to individual medical files. Before this can happen, the researchers must present their case before an ethics committee to check that their research is appropriate and worthwhile.

On rare occasions it is impractical to contact individuals for their consent, in which case the researchers must make their case before an ethics committee to show that there is enough benefit to the public at large to justify this.

The National Data Opt Out (objections to processing for secondary purposes)

The NHS Constitution states that "You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered".

In line with this there are choices you can make about how your information is used, and you can choose to opt out of your information being shared or used for any purpose beyond providing your care. The National Data Opt-Out Policy is a service that allows individuals to opt out of their confidential patient information being used for research and planning. It was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes.

The Hospice is one of many organisations working in the health and care system to improve care for service users and the public. Whenever you use a health or care service, such as attending Accident & Emergency or using Mental Health or Community Care services, important information about you is collected to help ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be provided to other approved organisations, where there is a legal basis, to help with planning

services, improving care provided, research into developing new treatments and preventing illness. All these helps to provide better health and care for you, your family and future generations. Confidential personal information about your health and care is only used in this way were allowed by law and would never be used for insurance or marketing purposes without your explicit consent.

You have a choice about whether you want your confidential information to be used in this way. If you are happy with this use of information you do not need to do anything. You can change your choice at any time.

To find out more about the wider use of confidential personal information and to register your choice to opt out if you do not want your data to be used in this way, visit <https://digital.nhs.uk/national-data-opt-out>. If you do choose to opt out, you can still consent to your data being used for specific purposes.

What are your rights over your personal data?

You have the following rights over your data we hold:

- **Subject Access Rights** – you can request access to and or copies of personal data we hold about you, free of charge (subject to exemptions) and provided to you within 1 calendar month. We request that you provide us with adequate information in writing to process your request such as full name, address, date of birth, Hospice EPR number and details of your request and documents to verify your identity so we can process the request efficiently. On processing a request, there may be occasions when information may be withheld if the organisation believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you. However, if the other person was acting in their professional capacity in caring for you, in normal circumstances they could not prevent you from having access to that information.

To request a copy or request access to information we hold about you and / or to request information to be corrected if it is inaccurate, please contact:

Executive Director of Strategy & Business Development
Queenscourt Hospice, Town Lane, Southport, PR8 5DY
Tel: 01704 517926
Email: hospice@queenscourt.org.uk

Right to rectification -The correction of personal data when incorrect, out of date or incomplete which must be acted upon within 1 calendar month of receipt of

such request. Please ensure the GP practice has the correct contact details for you.

- Right to withdraw consent -Where your explicit consent is required for any processing we do, you have the right to withdraw that consent at any time.
- Right to Erasure ('be forgotten') - This is not applicable to health records but is normally relied upon where consent is obtained for any processing. You have the right to have that data deleted / erased.
- Right to Data Portability - If we obtain consent for any processing we do, you have the right to have data provided to you in a commonly used and machine-readable format such as excel spreadsheet, csv file.
- Right to object to processing -You have the right to object to processing however please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If we didn't process any information about you and your health care it would be very difficult for us to care and treat you.
- Right to restriction of processing - This right enables individuals to suspend the processing of personal information, for example, if you want to establish its accuracy or the reason for processing it.

Where is your data processed?

Your data is processed within the Hospice and by other third parties suppliers. Where your data is processed and stored by our suppliers, for example the Hospice electronic patient record system (SystemOne), they must provide the Hospice with the relevant assurances that your data will be kept safe and securely. This is monitored by our Information Governance team.

Processing outside of the UK

The majority of the processing of your personal data is carried out in the UK. Where your data is processed outside the UK all suppliers and data processors as required to provide the Hospice with extra assurances that your data will be kept safe and in line with Data Protection legislation, specifically the UK GDPR. This may mean that they are asked to provide extra evidence.

Complaints / Contacting the Regulator

If you feel that your data has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, please contact our Caldicott Guardian/ IG Lead at the following contact details:

Email us at: hospice@queenscourt.org.uk

Or write to us at: Queenscourt Hospice, Town Lane, Southport, PR8 6RE

If you are not happy with our responses and wish to take your complaint to an independent body, you have the right to lodge a complaint with the Information Commissioner's Office.

You can contact them by calling 0303 123 1133

Or go online to www.ico.org.uk/concerns (opens in a new window, please note we can't be responsible for the content of external websites)

Data Security and Protection Toolkit

The Data Security and Protection Toolkit (DSPT) is an online assessment that must be completed every year by organisations who process Personal Data.

It is based on the National Data Guardian 10 Data Security Standards and also incorporates key requirements of the Data Protection legislation.

It measures whether an organisation is Data Protection compliant. Organisations are asked to provide evidence to show how they meet each standard.

The final assessment and evidence is normally submitted by 30 June each year and NHS England.

Queenscourt Hospice Information Governance Assessment Report (the DSPT) overall submission position for 2024-25 is 'standards met'.

Further Information / Contact Us

We hope that the Privacy Notice has been helpful in setting out the way we handle your personal data and your rights to control it. Should you have any questions / or

would like further information, please visit the websites below and / or contact either our Caldicott Guardian / Data Protection Officer at the following contact details:

Email us at hospice@queenscourt.org.uk

Or write to us at: Queenscourt Hospice, Town Lane, Southport, PR8 6RE

Further Information / Contact Us

We hope that the Privacy Notice has been helpful in setting out the way we handle your personal data and your rights to control it. Should you have any questions / or would like further information, please visit the websites below and / or contact either our Caldicott Guardian / Data Protection Officer at the following contact details:

Email us at: hospice@queenscourt.org.uk

Or write to us at: Queenscourt Hospice, Town Lane, Southport, PR8 6RE

Website: [Contact Us - Queenscourt Hospice](#)

Data Protection Officer: IG@midmerseyda.nhs.uk

Or write to the DPO at: Jubilee Court, Academy Site, Waterside, St Helens, WA9 1TT