HOSPICE IN THE WEALD

Celebrating Life, Dignifying Death

Data Protection Policy

POLICY NUMBER 6.10

Data Protection Policy

Document Detail	
Document type	*Policy*
Document name	*Data Protection Policy*
Internal / external	*Internal*
Document location	*Policy Hub on SharePoint*
Version	*1.0*
Effective From	*19/05/2025*
Review date	*19/05/2028*
Policy owner	*Sarah Winn*
Lead author	*David Bland*
Additional author(s)	
Applies to	
Approved by, date	*Information Sub Committee, 12/05/2025*

Change History		
Date	Change details since Approval	Approved by
12/05/2025	*Replacing GDPR Policy 6.10*	*Information Sub Committee*

Contents

1. Overview

Information Governance brings together the requirements and standards for handling Patient data. This includes Data Protection Legislation principles underpinned by the UK General Data Protection Regulation and the Data Protection Act 2018 (DPA2018), which set out the main responsibilities for the Hospice when we process Data.

To provide our range of services, the Hospice must collect Personal data, which will include special category data. We may collect information from a wide range of individuals, including but not restricted to, Patients, employees, volunteers, event organisers, donors, retail customers, business contacts and other health care providers.

The management of the information we hold is vitally important to assure our service users that we value and respect their information and to ensure we comply with the requirements set out in the data protection legislation.

Hospice in the Weald is committed to being concise, clear and transparent in how we obtain and process personal data and how we undertake these to the highest ethical standards We may occasionally be required to collect and use certain types of personal data to comply with the law.

The DPA 2018 provides an overview of the Hospice's approach to information governance and how the Hospice will meet the key requirements of a wide range of Information Governance related matters. It includes data protection related policies and details about the roles and management responsible for data security and protection in the Hospice.

2. Aims

This policy aims to support employees/information users in making decisions on the management of confidential information. It does not seek to provide for all eventualities but to raise awareness of where or from whom to seek further guidance.

This policy is to set out to promote a culture of good practice around the processing of information and use of systems that supports the provision of our high-quality care and services. This Policy will assist in the assurance that employees and all other information users will:

- establish good practice in the handling of information;
- promote a culture of awareness and improvement;
- comply with legislation and other mandatory standards.

It will also ensure that employees and all other information users understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access during their work. It covers:

- what is meant by personal data and special category data;
- how we obtain, use, share, secure and delete personal data and special category data in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g., about the personal data and special category data we gather and use about you, how it is used, stored and transferred, for what purposes, by whom and the steps taken to keep that information secure and for the time it is kept;
- your rights and obligations in relation to data protection;
- the consequences of failure to comply with this policy.

If you have any concerns about the content of this document, please contact the policy owner or advise the Policy Coordinator via policy.coordinator@hospiceintheweald.org.uk

3. Scope

This policy applies to all who process personal data for and on behalf of the Hospice. It will include employees, volunteers, contractors and any other individual who acts on our behalf. This group will be referred to as 'employees' throughout the policy.

4. Associated Documents

Privacy Notices
Subject Access Request policy
Information Sharing Policy
Information Risk Register
Records Management Policy

5. Key terms - abbreviations & definitions

Controller	A Controller determines the purposes and means of processing personal data – in most instances HitW will be the Controller
Processor	A processor is responsible for processing personal data on behalf of a controller. This occurs when we involve a third party in Processing data. When a third party is involved there must be a contract in place between the Controller and Processor.
Data Subject	An individual who is the subject of the personal data we hold.
Personal data	Data which relate to a living individual who can be identified from that data.
Special category data	Any data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
Processing	Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Any form of automated processing of personal data
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. The 'key' to unlocking the pseudonymisation must be kept separately and access controlled via technical organisational measures.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes.

6. Roles and responsibilities

6.1 Chief Executive

The Chief Executive has overall responsibility for Data and its management across the Hospice and is supported in this by the Trustees and the Information Governance Sub Commitee (IGSC).

Information Governance Sub Commitee (IGSC)
The IGSC will provide expert advice and guidance to all employees on all elements of Information Governance. The group may include, but need not be confined to:

- Information Governance Lead (IGL);
- Caldicott Guardian (CG);
- Senior Information Risk Officer (SIRO);
- Information Asset Owners (IAO); and
- Senior Management covering the key areas of the Hospice

6.2 Data Protection Officer

The Hospice is required to appoint a DPO. The DPO monitors internal compliance, provides advice regarding Data Protection Impact Assessments and is the contact point for Data Subjects and the supervisory authority, the Information Commissioner's Office.

The Hospice's nominated Data Protection Officer is BLS Stay Compliant, Blake House | 18 Blake Street | York | YO1 8QG. Registered Company: 9027319 | VAT Reg No: 191 0539 15

Responsibilities include informing and advising the Hospice and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Hospice's policies.

6.3 Senior Information Risk Owner (SIRO)

The SIRO will take ownership of the data risks the Hospice may face and will take responsibility for developing the culture and values the Hospice seeks to embrace. The SIRO will also report to the highest level of Hospice Management in order to ensure they are kept abreast of all risks to personal data and have an understanding of how such risks are being managed and mitigated.

6.4 Caldicott Guardian

The CG will be the Hospice's head of Clinical Services, who will act as the conscience of the Hospice. They will provide informed guidance about sharing data in the best interest of our Patients.

6.5 Information Asset Owners (IAO)

The IAOs will be responsible for ensuring that the data assets they own are managed appropriately, to meet the requirements of the Hospice, and that risks and opportunities are monitored and access to data controlled.

6.6 Managers

Managers are responsible for ensuring employee awareness of the implementation and application of all data policies, procedures and guidance. They will also ensure employees are supported in this aim.

6.7 Employees

Employees must be aware of and adhere to all policies, procedures and guidance advised within this document. You must read, understand and comply with this Policy when processing personal data on behalf of the Hospice and attend training on its requirements. Any breach of this Policy may result in disciplinary action. Up to and including dismissal.

7. Data Protection and Confidentiality compliance

Good practice requires that the Hospice has in place processes to highlight actual or potential confidentiality breaches and poor adherence to guidelines and procedures designed to ensure compliance. To that end, we have in place policies and procedures to evaluate the effectiveness of controls.

This ensures that all processing within the Hospice is not only guided by policy, but there are also checks in place to ensure that processes are audited in an appropriately structured way.

This function will be co-ordinated by the Information Governance Sub Committee through a programme of audits.

8. Consequences and implications of failing to comply

The Hospice takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal data is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and the Hospice; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

9. Data protection principles

The UK General Data Protection Regulation (UK GDPR) was approved in 2018. The U K GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018)
The Hospice, as a Data Controller, must comply with the seven Data Protection Principles set out in within UK GDPR. In summary, these state that personal data shall be:

I. Processed lawfully, fairly and in a transparent manner in relation to individuals.
The DPA 2018 restricts our data processing actions to specified lawful purposes to ensure we process data in a way which will not adversely affect the Data Subject.

This principle is covered within our Privacy Notices which detail everything we will do with the personal data collected on behalf of our service users, whilst we process it on their behalf.

II. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

The Hospice cannot use personal data for alternatively legitimate purposes from the original reason, unless we have informed the Data Subject of the new purposes and they have consented where necessary.

III. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

You may only collect and/or process personal data which is needed to perform your job duties. This will mean that you, whilst carrying out your tasks, only process the smallest amount of personal data for the intended purposes.

IV. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which they are processed.

Data should be rectified without delay ('accuracy'). You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

V. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for; archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation').

VI. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

VII. Article 5(2) goes on to add Accountability. The controller shall be responsible for, and be able to demonstrate compliance with all of the principles above, which covers the requirement for all Hospices to be able to demonstrate their accountability.

10. Caldicott principles

In addition to the provisions of UK GDPR and the DPA 2018, the Hospice also adheres to the principles which arose from the Caldicott Reports, which underpin the fundamental rules and regulations that guide a patient's confidentiality. They are the basic rules every healthcare personnel must follow to ensure there is no breach of confidentiality whatsoever.

- **Principle 1**: Justify the purpose(s) for using confidential information;
- **Principle 2**: Use personal confidential data only when it is necessary;
- **Principle 3**: Use the minimum necessary personal confidential data requirements to meet your aim;
- **Principle 4**: Access to personal confidential data should be on a strict need-to-know basis and restricted to those who should have access to it;
- **Principle 5**: Everyone with access to personal confidential data should be aware of their responsibilities;
- **Principle 6**: Comply with the law;
- **Principle 7**: The duty to share information can be as important as the duty to protect patient confidentiality.

- **Principle 8:** Inform patients and service users about how their confidential information is used.

11. Data

11.1 What data do we collect and hold about our service users?

We may collect a wide range of information, including but not limited to; name and all contact details, medical history, next of kin, donor information, health care preferences, religious belief, bank details and any special considerations around support they may require.

The information we hold relating to our service users, which we process to provide our services, falls into two distinct categories. Personal Data and Special Category Data.

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

11.2 Personal Data

Personal data is information relating to living persons who can be identified, or who are identifiable, directly from the information we are processing, or who can be identified from that information in combination with other information.

The Information Commissioner's Office refers to a name as being the most common means of identifying someone. Whether any potential identifier identifies an individual depends on the context, a combination of identifiers may be needed to identify an individual.

The UK GDPR provides a non-exhaustive list of identifiers, including:

- name;
- identification number;
- location data; and
- an online identifier. 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.

11.3 Special Category Data

Sensitive personal data is known as Special Category Data. Special category data is personal data that needs more protection because it is sensitive and the risk to the data subject is considered to be greater if there should be any data breach or incident involving the data.

The UK GDPR defines special category data as personal data:

- revealing racial or ethnic origin;
- revealing political opinions;
- revealing religious or philosophical beliefs;
- revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- concerning health;
- concerning a person's sex life; and sexual orientation.

12 Lawful Basis for processing personal data

The first principle under Article 5 requires that you process all Personal data, whether personal data or special category data, lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis to apply to the processing undertaken for the Hospice.

If no lawful basis applies to our processing, the processing will be unlawful and in breach of the first principle. Individuals have the right to erase personal data which has been processed unlawfully.

There are six lawful bases we can use to process Personal Data. When selecting the correct basis, the choice will be from UK GDPR Article 6, which outlines the following reasons for processing:

(a) **consent**: the individual has given clear consent for you to process their personal data for a specific purpose;
(b) **contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
(c) **legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations);
(d) **vital interests:** the processing is necessary to protect someone's life;
(e) **public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;
(f) **legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

To choose the correct legal basis you should consider why you want to process the data and select the appropriate basis. If you have difficulty assigning a lawful basis, you should talk with your line manager or the Hospice SIRO.

A further note on consent as it relates to the Hospice

Consent means offering individuals real choice and control. Genuine consent should put our data subjects in charge, build customer trust and engagement, and present an opportunity to enhance our reputation. The UK GDPR sets a high standard for consent, occasionally consent won't be needed.

If consent is difficult or inappropriate, look for a different lawful basis.

If Consent is used as a lawful basis the data process owner must ensure that the process for asking for consent is specific, informed and unambiguous so that we can be confident that consent is being freely given. This can be achieved by ensuring that we:

- don't use pre-ticked boxes or any other type of default consent.
- use clear, plain language that is easy to understand.
- specify why we want the data and what we're going to do with it.
- give individual ('granular') options to consent separately to different purposes and types of processing.
- name our Hospice and any third-party controllers who will be relying on the consent.
- tell individuals they can withdraw their consent.
- ensure that individuals can refuse to consent without detriment.
- avoid making consent a precondition of a service.

There is no set time limit for Consent.

At Hospice in the Weald the most common reason for using Consent as a lawful basis will be when seeking permission for Hospice in the Weald to use personal and recorded material for marketing and communications purposes.

Appendix 3 sets out the form for obtaining Consent for this purpose. Scans of completed forms should be saved to EMIS and the Fundraising database.

13 Lawful Basis for processing special category data

The Hospice recognises that Special Category Data requires additional protection, as it has the potential to reveal sensitive aspects relating to the data subject. This means that if you process any special category details on behalf of the Hospice a second level of protection must be assigned. The conditions applicable to Special Category Data are outlined in UK GDPR Article 9.

They are:

(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)

If relying on conditions (b), (h), (i) or (j), you must also meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

Before processing any sensitive personal data, staff must notify the Data Protection Officer and the Information Governance lead of the proposed processing, so they may assess if the processing complies with the criteria noted above.

Special category data will not be processed until:

- the assessment above has taken place; and
- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

In relation to sensitive personal data, the Hospice will comply with the procedures set out in this policy to make sure that it complies with the data protection principles.

14 Third party processing

HitW is the data controller for personal and sensitive data that is collected during its activities, for the purposes set out above. On occasion, a third-party organisations may process the Hospice's data as part of a contracted-out service.

It is a legal requirement that contracts or service level agreements relating to third party processing activity include clauses setting out the controller's and processer's (third party) obligations. The SIRO is responsible for ensuring these are inserted into contracts and agreed by both parties.

15 Surveillance cameras

Several Closed-Circuit TV (CCTV) cameras are on Hospice premises to assist with security for staff, other individuals and their property. Images and audio recording obtained through CCTV are considered personal data and will be treated as such.

If a request is received under an individual's right of access, images and audio will be treated with the same consideration as other personal data.

Requests for images from the CCTV system will be controlled and consistent with the system's purpose.

Subject to appropriate documentation in support of a request, it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, it would not be considered appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

If you have any queries regarding the operation of, or access to the CCTV system, please contact the Hospice's SIRO. If access is required in connection with ongoing disciplinary matters, permission should be sought from the Director of People and Culture.

16 Individuals Rights

UK GDPR stipulates that all individuals who have their data processed by an organisation have certain rights as to how that data is processed and what may be done with it. These individual rights are listed below and all apply to every data subject.

Right to be informed

The right to be informed encompasses obligations to provide 'fair processing information', typically through a privacy notice. The information supplied about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Right of access

Under the UK GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information

Right of rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. In instances where data has been disclosed to third parties, we will be required to contact each third party and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

Individuals are entitled to know which third parties their data has been disclosed to.

Right of erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the UK GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply. A request for erasure may be denied if the following circumstances apply:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims

Right to restrict processing

Individuals can request a restriction on the processing of their personal data in the following circumstances:

- When an individual contests the accuracy of data that we hold about them.
- Where an individual has objected to the processing and we are considering whether our Hospice's legitimate grounds override those of the individual.
- When processing is unlawful, and the individual opposes erasure and requests restriction instead.
- If HitW no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Right to data portability

The right to data portability applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

Right to object to processing

Individuals have the right to object to:

- processing based on legitimate interests
- direct marketing (including profiling); and

- processing for purposes of scientific/historical research and statistics.

When individuals object we must stop processing their personal data

Rights related to automated decision making

For something to be solely automated there must be no human involvement in the decision-making process. The restriction set by this Right only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

HitW does not carry out any solely automated decision making.

17 Privacy notices

The Privacy Notice is available on our website and within the Hospice as required. A hard copy is available. The privacy notice applies to the websites, products and services offered by the Hospice.

For employees and also for our volunteers, the Hospice will issue privacy notices informing you about the personal data that we collect and hold relating to you. You will be advised if there are updates.

When collecting information for specific activities such as event entry and registration, regular giving etc. an appropriate information notice will be displayed.

We will take appropriate measures to provide information in privacy and information notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

18 Data Protection Impact Assessments

Where processing is likely to result in a high risk to an individual's data protection rights (e.g., where the Hospice is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals;
- what measures can be put in place to address those risks and protect Personal data.

This privacy by design and default approach ensures that before any new form of technology is introduced, the manager responsible should contact the Data Protection Officer so that a DPIA can be done.

Full procedural guidelines for conducting a DPIA can be found within the **Information Sharing Policy**.

19 Documentation and Record management

We record the processing life cycle of data on a Record of Processing Activity, (ROPA). This ensures that for every aspect of processing which may potentially impact on the rights of the individual, we have clarity at any given

point as to how the data is being processed.

The ROPA includes:

- what data is included in the processing;
- the purposes of the processing;
- a description of the categories of individuals whose data is involved and categories of personal data;
- details of the recipients of the personal data;
- the Hospice does not operate in more than one EU member state and whilst the Hospice does not carry our cross-border processing in its role as Controller, it is acknowledged that data may be processed via Third Party suppliers or processors. Any data for which the Hospice is Controller, when processed further, will be subject to Data Processing Agreements to ensure data security is equal to our own. Any information on Data Subjects who reside outside the UK will be held to the same processing standards as all EU processing;
- retention schedules;
- a description of technical and organisational security measures.

As part of our ROPA we also document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- relevant DPIAs
- records of data breaches and near misses which involve the data asset.

When we process Special Category Data or criminal records information, we will keep records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for our processing;
- whether we retain and erase the personal data in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal data we process and update our documentation accordingly. This may include:

- carrying out information audits to find out what Personal data the Hospice holds;
- distributing questionnaires and talking to staff across the Hospice to get a more complete picture of our processing activities;
- reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

The results of this mapping exercise will be retained with the associated risks included in the **Information Risk Register** for appropriate action.

20 Information Security

The Hospice will use appropriate technical and organisational measures to keep data secure, and to protect against unauthorised or unlawful access whether intentional or unintentional, processing and accidental loss, destruction or damage.

These may include, but are not limited to:

- making sure that, where possible, Personal data is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring electronic backups are run regularly;
- all equipment used to process data electronically has processing capability to be backed up;
- ensuring that in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner;
- regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for the security of the processing is in place.

Where the Hospice uses external partners to process personal data additional security arrangements need to be implemented in contracts with those partners to safeguard the security of Personal data. Contracts with external Processors must include:

- details of the processing to be completed;
- that those processing the data are subject to a duty of confidentiality;
- assurance that all personnel have been trained adequately in Information Governance;
- details of the appropriate measures being taken to ensure the security of processing;
- agreement that sub-contractors are only engaged with the prior consent of the Hospice and under a written contract;
- reassurance the Processor will assist the Hospice in fulfilling subject access requests and allowing individuals to exercise their rights under Data Protection regulations;
- confirmation that the Processor will assist the Hospice in meeting its Data Protection obligations in relation to the notification of data breaches and data protection impact assessments;
- that the Processor will delete or return all personal data to the Hospice as requested at the end of the contract; and provide evidence to confirm this;
- surety that the Processor will submit to audits and inspections, provide the Hospice with whatever information it needs to ensure that they are meeting their data protection obligations, and inform the Hospice immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of Personal data by an external Hospice is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer and a DPIA be considered if relevant.

21 Individual obligations

All individuals authorised to process data for the Hospice are responsible for adhering to the standards expected. This includes ensuring the data the Hospice holds which relates to them as an individual is accurate. You should let the HR team know if the information you have provided to the Hospice changes, for example if you move house or change details of the bank or building society account to which you are paid.

The Hospice expects you to help meet its data protection obligations when handling and processing all data.

It is forbidden, on any of the systems used for accessing and processing personal data, for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

The Hospice may, if there is due cause to suggest a breach, monitor the use of Hospice equipment. You will be notified before this is carried out unless there is involvement through law enforcement reasons. You may not be informed if this is the case.

If you have access to Personal data, you must:

- only access the personal data that you have authority to access, and only for authorised purposes;
- only allow other Hospice employees and volunteers to access personal data if they have appropriate authorisation;
- only allow individuals who are not Hospice staff to access personal data if you have specific authority to do so from the Information Governance Lead;
- keep Personal data secure (e.g., by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Hospice's policies);
- not remove personal data, or devices containing personal data (or which can be used to access it), from the Hospice's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device;
- not store personal data on local drives or on personal devices that are used for work purposes.

You should contact the Information Governance Lead if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing;
- any suspected or actual data breach;
- access to personal data without the proper authorisation;
- personal data not managed or deleted securely;
- removal of Personal data, or devices containing Personal data (or which can be used to access it), from the Hospice's premises without appropriate security measures being in place; and
- any other breach of this Policy or of any of the data protection principles set out above.

22 Audit and training

All Hospice personnel will be required to undergo mandatory data privacy related training which the Hospice will provide periodically. The Hospice will maintain a record of training attendance by all personnel.

All staff will have a level of awareness and training appropriate to their role.
Knowledge of basic data protection principles will be:

- Part of all induction and orientation.
- A requirement to pass the probationary period.
- Reviewed every 1 years via the mandatory training e-learning requirements.
  Additional training will be provided for those in IG (Information Governance) roles e.g. Caldicott Guardian, Data Protection Officer, SIRO and IOAs.

23 Data breaches and incident management

All breaches of data protection must be reported as an incident to the relevant Information Asset Owner or to your Line Manager in the first instance.

All data protection/IG incidents will be managed through our incident policy and process.

A personal data breach means,

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than about losing personal data." (ICO)

Data breaches that pose a risk to the rights and freedoms of individuals need to be reported to the Information Commissioner's Office within 72 hours by the Data Protection Officer.

If data breaches pose an elevated risk to the rights and freedoms of individuals, they need to be communicated to the individual directly.

In assessing the risks, the following need to be considered:

- The type of breach e.g., there will be different consequences between whether data is lost compared to unauthorised disclosure;
- The nature, sensitivity and volume of personal data e.g., breach of medical information will have a different impact to disclosure of the name of a staff member;
- Ease of identification of individuals;
- Severity of consequences e.g., could the breach lead to fraud or theft, humiliation, or reputational damage?
- Special characteristics of the individuals e.g., are children or vulnerable adults particularly affected;
- Number of affected individuals.

Breaches in confidentiality by staff will be managed through the disciplinary process and according to policy.

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which Personal data is stored;
- unauthorised access to Hospice systems by information users;
- unauthorised access to or use of Personal data by an information user or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- disclosure of personal or confidential information to a third party where there is no justification and there are concerns that it is not in accordance with regulations;
- sending of personal or confidential information in a way that breaches confidentiality;
- leaving of personal or confidential information in public areas;
- disposal of personal or confidential information in public areas in an unsecured manner;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the Hospice which holds it.

In line with the expectation of the Information Commissioner's Office the Hospice will report all data breaches without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals.

To determine if a breach is reportable, the individual managing the breach will access Self-assessment for data breaches | ICO where it can be determined if reporting should take place.

When it has been decided to report a breach the member of the IG Group will notify the affected individuals. This is especially important if a data breach is likely to result in a high risk to their rights and freedoms where notification is required by law.

24 Direct marketing

A Data Subject's prior consent is required for electronic direct marketing (for example by email, text or automated calls).

You must promptly honour a Data Subject's objection to direct marketing and if a service user opts out at any time, their details must be suppressed as soon as possible.

HitW offer an 'opt out' / 'unsubscribe' option with all our electronic marketing, as well as a direct Privacy email inbox where this can be requested, that is monitored by the Information Governance Lead.

25 Disclosure, sharing and transfer of personal data

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check there is legitimate basis for access to the information before releasing it.

It is important to consider how much information is needed before disclosing it and only the minimal amount necessary is disclosed. If anyone has any concerns about disclosing any information, they must discuss this with their line manager or a member of the Information Governance Group.

Data protection regulations entitle an individual, with certain exceptions, to a copy of both manual data recorded in a relevant filing system and computer data relating to them that is held by a third party together with information as to why it is being processed and the sources and destination of the data. There is no time restriction as to when the record was created.

A request for such information under the Act is known as a Subject Access Request and are managed by the Caldicott Guradian

Where individuals are applying for access to a deceased person's records the Access to Health Records Act 1990 applies.

26 Storage and retention of personal data

All data regardless of category will be kept securely in accordance with the highest standards required by Data Protection legislation and in accordance with the Hospice retention schedule which sets out the relevant retention period.

Where there is any uncertainty, staff should consult the Data Protection Officer.

Information which permits identification of data subjects will be kept for no longer than is necessary for the purposes for which the personal data are processed and we will:

- follow retention guidelines in the Records Management Policy;
- ensure regular weeding of data;
- refrain from adopting the "just in case it might be useful one day" philosophy;
- follow disposal policy and procedures.

Personal data should not be retained for any longer than necessary. Data retention will depend upon the circumstances, including the reasons why the personal data was obtained.

27 Monitoring and review

Adherence to this policy will be monitored and failure to follow the guidelines within the Policy may result in disciplinary action.

The Policy will be subject to regular review as detailed in the Policy matrix and also in the following circumstances.

- In response to data breaches or incidents relevant to this Policy.
- Where best practice indicates change would be beneficial.
- When there are changes to legal guidance or regulatory requirements.

27 Equality impact screening tool

- This screening tool must be completed at the start of any new or existing policy or procedure development. All sections of the tool will expand as required.

Section 1	
Protected Characteristic	**If the proposal/s have a positive or negative impact, please give brief details**
Age	N/A
Disability	N/A
Gender reassignment	N/A
Marriage or civil partnership	N/A
Pregnancy and maternity	N/A
Race	N/A
Religion or belief	N/A
Sex	N/A
Sexual orientation.	N/A
Other underserved communities (Including Carers, Low Income,	N/A

Section 2

Will implementation of this policy / procedure have a <u>significant</u> <u>adverse</u> impact for people with protected characteristics or otherwise listed above, in relation to <u>any</u> of the following six categories? Please mark in the yes/no checkbox below, as appropriate.

NB: In this context 'significant' means that potential adverse impacts of implementing the policy can <u>not</u> be mitigated against within the policy / procedure itself.

1. Adversely affect patient safety or clinical effectiveness
2. Adversely affect compliance with statutory/regulatory requirements e.g. NICE requirements, CQC, Equality Act, Care Act etc.
3. Adversely affect the experience of a patient or their loved one(s)
4. Adversely affect the experience of staff or volunteers
5. Adversely affect access to Hospice services

Yes		No	
High risk: Complete further Equality Impact Assessment (EqIA) tool, available from the Policy Co-ordinator policy.coordinator@hospiceintheweald.org.uk	**[ ]**	Low risk: Go to section 3.	**[X]**

Section 3

If this proposal is low risk, please give evidence or justification for how you reached this decision:

This policy offers insight and guidance around how we protect our own, as well as our service users, data and offers a low risk of impacting on the equality

Signed by Policy / Procedure Lead Author		**Date**	
Sign off that this proposal is low risk and does not require further EqIA			
Signed by EDI Lead		**Date**	