Policy and Procedure: **General Data Protection Regulations**
Policy number: **6.10**

1. Policy Statement

Hospice in the Weald is committed to robust data protection measures. This policy sets out our approach to compliance with the General Data Protection Regulations, and the responsibilities for staff and volunteers. This Policy should be viewed in conjunction with the GDPR tracker which is a live document, stored on Hospice Web.

2. Related policies, guidelines and procedures

4.1	Patient Access to Health Records
4.2	Health Records: Management of Patient Records
4.5	Patient Identification
4.8	Copying Letters to Patients
4.9	Health Records – Data Sharing
6.11	Consent to Care
12.1	Information Communication Technology (ICT)
12.2	Remote, Removable and Mobile ICT

3. Responsibility and Accountability

Policy formulation and review:	Income Generation Director via HLT
Approval:	CEO
Compliance:	All staff and volunteers

4. Relevant Dates

Policy originated:	April 2018
Date of last review:	April 2019
Date of next review:	April 2021

CONTENTS

Introduction	Page 3
Key Terms	Page 3
6 Principles of GDPR	Page 4
Lawful basis for processing personal data	Page 5
Special category data	Page 8
Criminal offence data	Page 8
Choosing the 'right' lawful basis	Page 8
The Data Subject's rights	Page 9
Contracts	Page 11
Data protection by design and default	Page 12
Data protection impact assessments	Page 12
Data protection officers	Page 13
Codes of conduct and certification	Page 13
Security	Page 13
International transfers	Page 14
Personal data breaches	Page 14
Children	Page 14
Appendix 1 - Specific conditions applying to the processing of special category data	Page 15
Appendix 2 – summary of the information that should supplied in discharging the Right to be Informed	Page 16
Appendix 3: Consent for Use of Personal and Recorded Material	Page 17

INTRODUCTION

The General Data Protection Regulations (GDPR) came into force on 25th May 2018:

- The new rules will apply to all businesses regardless of size
- GDPR is significantly more demanding than existing rules
- Fines for non-compliance will be up to 20M Euros or 4% of turnover

Whilst the above may all be true the GDPR presents an opportunity to streamline our data handling processes, resulting in:

- Improved service to supporters, customers, patients, families and caregivers
- Reduced costs
- Reduced risks

As part of good data management in line with GDPR, all mailings from Hospice in the Weald should be sent from Raisers Edge to ensure the most accurate information is used, with the exceptions of individual letters relating to clinical or employment matters which may be sent from EMIS or ADP respectively.

KEY TERMS

In the context of GDPR some words have specific meanings, which may be quite different to the everyday use

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	A person to whom personal data belongs to
Personal Data	Any information relating to an identified or identifiable natural person (the 'Data Subject')
Sensitive personal data	Any data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. Sometimes referred to as "special category data".
Processing	Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, 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 and organisational measures.

Consent	means any **freely given, specific, informed** and **unambiguous** indication of the data subject's wishes. Note that the **highlighted** words have specific connotations in GDPR, more on this later.

SIX PRINCIPLES OF GDPR

The regulations require that the Controller be responsible for, and be able to demonstrate, compliance with the principles that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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 GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

LAWFUL BASIS FOR PROCESSING PERSONAL DATA

The principles listed above lead to the lawful basis for Processing data. We must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual. Most lawful bases require that processing is 'necessary'. If we can reasonably achieve the same purpose without the processing, we don't have a lawful basis.

The lawful basis which we are using to process data must be determined before the processing begins. It is good practice to document the lawful basis being used in relation to specific data processing activities, especially as there is a mandatory requirement to record processing purposes, data sharing and retention practices. The GDPR tracker combines all this information in one place.

- **Consent**

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and presents an opportunity to enhance our reputation. The GDPR sets a high standard for consent, but often consent won't be needed. If consent is difficult, 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 organisation 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.

Explicit consent must be expressly confirmed in words, rather than by any other positive action. 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.

- **Contract**

This lawful basis can be used when we need to process someone's personal data:

- to fulfil a contractual obligation to them; or
- because they have asked us to do something before entering into a contract (e.g. apply for a job).

The lawful basis for processing necessary for contracts is almost identical to the old condition for processing under the Data Protection Act 1998

- **Legal obligation**

Rely on this lawful basis when it is necessary to process personal data to comply with a common law or statutory obligation. This does not apply to contractual obligations. For example: as an employer HitW needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC. The lawful basis for processing necessary for legal obligation is almost identical to the old condition for processing under the Data Protection Act 1998

- **Vital interests**

Rely on vital interests as a lawful basis when it is necessary to process personal data to protect someone's life. The lawful basis for vital interests is very similar to the old condition for processing in the 1998 Act. One key difference is that anyone's vital interests can now provide a basis for processing, not just those of the data subject themselves.

When 'vital interests' is used as a lawful basis there will generally be an immediate threat to life, for medical care that is planned in advance another lawful basis such as public task or legitimate interests is likely to be more appropriate.

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the special categories of data, which means it will also be necessary to identify a condition for processing special category data.

- **Public Task**

Rely on this lawful basis when it is necessary to process personal data in order to perform a task in the public interest or to carry out official functions, and the task or function has a clear basis in law. The GDPR is clear that public authorities can no longer rely on legitimate interests for processing carried out in performance of their tasks. For this reason, it is likely that the NHS will use 'Public Task' as the lawful basis for many data processing activities. HitW is not a public authority.

In this guide the term 'public task' is used to help describe and label this lawful basis. However, this is not a term used in the GDPR itself. When determining whether to use this lawful basis the focus should be on demonstrating either that we are carrying out a task in the public interest, or that we are exercising official authority.

- **Legitimate interests**

Legitimate interests is the most flexible lawful basis for processing, but it must not be assumed it will always be the most appropriate. It is likely to be most appropriate when people's data is being used in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing.

To rely on legitimate interests, we must be able to demonstrate that we are taking on extra responsibility for considering and protecting people's rights and interests. The legitimate interests can be our own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. Our interests must be balanced against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override our legitimate interests.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. We can rely on legitimate interests for marketing activities if we can show that the use of people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object. Use of email address or mobile telephone number will require **specific opt-in consent** as part of the Privacy and Electronic Communications Regulations.

When relying on legitimate interests, consider the points listed below. If you think that the legitimate interests may be contested then consider recording this in a separate document and linking it to the GDPR Tracker.

First, identify the legitimate interest(s):

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?

- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

SPECIAL CATEGORY DATA

Special category data includes, but is not limited to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Specific conditions apply to the processing of special category data, these are set out in Appendix 1.

CRIMINAL OFFENCE DATA

To process personal data about criminal convictions or offences requires having both a lawful basis and either legal authority or official authority for the processing. This means either processing the data in an official capacity or having specific legal authorisation. This is covered under the Data Protection Bill, not the GDPR.

CHOOSING THE 'RIGHT' LAWFUL BASIS

When data processing occurs for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases there is likely to be a choice between using legitimate interests or consent. To determine which is the 'right' lawful basis to use consideration should be given to the wider context, including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is our relationship with the individual?
- Could it be considered that we are we in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are we able to stop the processing at any time on request?

Using legitimate interests as a lawful basis allows us to keep control over the processing but means that we must take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, using Consent gives individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed).

THE DATA SUBJECT'S RIGHTS

- **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.

Appendix 2 summarises the information that should supply to individuals and at what stage.

- **Right of access**

Under the 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 to 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 to 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 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. Aa 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 organisation'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 only 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**

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 including profiling**

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.

CONTRACTS

Whenever a Controller uses a Processor it needs to have a written contract in place. These contracts must include certain details and specific terms, as a minimum. These terms are designed to ensure that Processing carried out by a Processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).

The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors - though none have been drafted so far(!).

The most practical way of ensuring an appropriate contract is in place when working with a Processor is to ask the Processor to confirm in writing that their work is compliant with the GDPR. The person from HitW who is signing the contract should then check that the following terms are included:

Our contracts must include the following compulsory details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;

- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Our contracts must include the following compulsory terms:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

DATA PROTECTION BY DESIGN AND DEFAULT

Measures could include:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing; and
- creating and improving security features on an ongoing basis.

DATA PROTECTION IMPACT ASSESSMENTS

Data protection impact assessments (DPIA) are a tool which can help identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. At HitW the most likely scenario when a DPIA would be required would be as part of a project, or some other significant undertaking, which included making significant changes to data Processing e.g. implementing a new patient records system. A DPIA must be undertaken when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.
- This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
- large scale, systematic monitoring of public areas (CCTV).

DATA PROTECTION OFFICERS

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances. A DPO must be appointed when an organisation:

- is a public authority (except for courts acting in their judicial capacity);
- carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

The guidance is not clear on whether HitW would be required to appoint a DPO, however we have decided to incorporate the function of DPO into the Head of Communications job description. The Head of Communications will:

- Inform and advise HLT about our obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities; advise on data protection impact assessments; train staff, and conduct internal audits.
- Be the first point of contact for supervisory authorities and for all external individuals whose data is processed (supporters, customers etc).

CODES OF CONDUCT AND CERTIFICATION

Signing up to a code of conduct or certification scheme is not obligatory, but it is recommended.

There is a low level of awareness of the new Fundraising Regulator amongst the general public and for this reason we will not, at the present moment, register with the Fundraising Regulator.

The NHS has yet to publish Information Governance guidance relating to GDPR. Although we are not part of the NHS we will reflect their guidance in our approach, where relevant.

SECURITY

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used. The GDPR Tracker include a section on data security.

INTERNATIONAL TRANSFERS

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

PERSONAL DATA BREACHES

The GDPR introduces a duty to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals most also be informed without undue delay.

Internal monitoring/auditing will be required to ensure we have robust breach detection, investigation and reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

A record must be kept of any personal data breaches, regardless of whether we are required to notify.

CHILDREN

The GDPR states that, if Consent is the lawful basis being used to process a child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility'. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing.

Appendix 1 - Specific conditions applying to the processing of special category data

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2 – summary of the information that should supplied in discharging the Right to be Informed

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Appendix 3: Consent for Use of Personal and Recorded Material

This form is an appendix off our General Data Protection Regulations Policy (Policy number 6.10). If you would like to see that policy before giving your Consent, please ask any member of staff or volunteer who will be happy to provide you with a copy.

By giving permission for the following personal and recorded material you give permission for Hospice in the Weald to use the personal and recorded material for marketing and communications, including: internal communications with our workforce; patient, family and carer literature; training and development; fundraising publications (for example the newsletter, local newspapers, our website, social media where it is possible for members of the public to also share content).

Please note, this consent is **not** time limited, but Hospice in the Weald will always endeavour to use current material when creating new literature. Once material is released, however, it cannot be recalled. We would encourage you to share with your loved ones and next of kin that you have given us consent for use of your personal or recorded material.

Please find below a list of types of personal and recorded material and indicate by ticking, which types you would like to be used for any of the above purposes. If you do not wish the recorded material to be used, then please leave blank.

Photographs of Yourself	☐
Creative Artwork	☐
Video / voice recordings, including the 'Informed Guide'	☐
Other (Hospice Voice story etc.)	☐

If other, please give details ……

Signature…… **Date**……

Name (in capitals letters please) ……

If signing on behalf of a minor (under 18) please state minor's name here……

Name of workforce member completing this form……

For Hospice workforce to complete – record details of person giving Consent

Address: DOB:

Contact telephone number:

Donorflex / Raiser's Edge ID: EMIS number: