Woking & Sam Beare
Hospice and Wellbeing Care

`

DATA PROTECTION AND CONFIDENTIALITY POLICY

Policy / procedure code:	IG02
Version:	V2
Policy owner:	SIRO
Approval Date:	19 Aug 2022
Ratified by:	Governance Committee
Next Review Date:	Aug 2025
For Information and action to:	Employed staff, Trustees and Volunteers, Staff placements, Locums and Agency staff, Contractors and third parties

Version Control Sheet

Policy / Procedure: Data Protection and Confidentiality Policy

Version	Date	Author	Status	Comment
V1.1	Nov 2017	B Hamilton	Approved	Major Review – incorporate organisation wide standards and GDPR references
V2	Jun 2022	J Gardner	Draft	Full Review and update Reviewed and recommended for approval by Information Governance Lead, SIRO, CEO and Director of Clinical Services
V2	19/08/22	N/A	Approved	Governance Committee

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version on the R Drive is the controlled copy. Any printed copies of this document are not controlled. As a controlled document this document should not be saved onto another Drive and should only be accessed from the Resources Folder: Resources Site \ Policies & Guidelines \ Information Governance

Contents **Page**

1. Introduction

Data is central to the way Woking and Sam Beare Hospice (WSBH) enables effective care and treatment of patients and how it plans its resources. Personal data belonging to patients, employees, volunteers, supporters and customers is one of its most important assets in providing all services.

The Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR) sets out the legal framework by which WSBH can process personal information safely and securely. It operates alongside the common law duty of confidentiality which governs information given in confidence to health professionals with the expectation that it will be kept confidential.

The UK GDPR sets out seven data protection principles which describe the legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the seven data protection principles is unlawful.

As a data controller, WSBH is responsible for ensuring and demonstrating compliance with the UK GDPR.

The DPA Act 2018 applies only to information relating to living individuals. The Common Law Duty of Confidentiality, however, ensures that a patient's right to confidentiality continues after their death.

The Hospice is required to register annually with the Information Commissioner's Office (ICO), which is the UK's independent body set up to uphold information rights. The Hospice's unique registration numbers are ZA 088704 (Woking) and ZA008714 (Sam Beare).

WSBH is mandated to complete a self-assessment tool to measure its performance against the 10 data security standards set out by the National Data Guardian. The Data Security and Protection Toolkit (DSPT) is used to measure compliance (Appendix 1).

Data protection and confidentiality are components of Information Governance and this policy forms part of the Information Governance Framework (IG01). This Policy should, therefore, be read in conjunction with all relevant policies, standard operating procedures (SOPs) and guidance within the Framework that cover the use and security of information (Appendix 2).

2. Purpose

This policy sets out the requirements for processing data in an effective and secure manner which complies with current legislation and best practice relating to data protection and confidentiality.

The Policy will promote best practice for processing personal data to ensure that WSBH staff, Trustees, volunteers, contractors and third parties understand both the Hospice's and their own personal responsibilities when handling personal data.

3. Scope

This Policy applies to all personal data obtained and processed by Hospice staff which is held electronically, in manual paper-based filing systems and in other formats. This data includes, but is not limited to the following:

- Patient, client, service user, customer and supporter information
- Employee personal information
- Clinical research, audit and reporting information

This policy applies to all Hospice and non-Hospice employees who process personal data to perform their role or who handle data on behalf of the Hospice including:

- Employed staff (including Bank staff and staff on fixed or temporary contracts)
- Trustees and Volunteers
- Staff placements (students, medical staff and allied healthcare professionals)
- Locums and Agency staff
- Contractors and third parties

From this point forward the term 'staff' refers to all employed and non-employed staff.

4. Roles and Responsibilities

Roles	Responsibilities
Board	• Ensures there is an effective programme for Information Governance and assurance in place • Ensures sufficient resources are provided to support policy requirements
Chief Executive	• Overall accountability for data security and protection and compliance with the applicable legislation and regulations
Governance Committee	• Provides assurance on data protection and security to the Board and manages the relevant risks and issues that are escalated by the Management Team
Management Team	• Development and implementation of Information Governance and related Policies • Ensures compliance and sign off of the Data Security and Protection Toolkit (DSPT) providing assurance of meeting key standards. • Development and implementation of robust improvement plans to address any DSPT non-compliance • Ensures that information risks are assessed and mitigated to an acceptable level and handled in a similar manner to other major risks such as financial, legal and reputational risks

Roles	Responsibilities
	• Reviews serious incidents involving actual or potential loss of personal data or breach of confidentiality which must be published in annual reports and to the ICO.
Senior Information Risk Owner (SIRO)	• Hospice compliance with Information Governance Management and advises the Board on the effectiveness of information risk management and risk issues • Authorises the submission of the Data Protection and Security Toolkit
Caldicott Guardian	• Protects the confidentiality of patient and service user information and enables appropriate information sharing • Champions IG requirements and issues at the Board and Management Team meetings • Considers and approves, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures.
IG Leads / IT Manager	• Oversees the IG requirements for WSBH on a day-to-day basis and ensures appropriate systems and processes are in place to support adherence to standards • Leads the delivery of the IG Improvement Plan • Completes the allocated components of the DSPT within the required timeline for the annual assessment • In support of the SIRO ensures that Information Asset Owners (IAOs) are nominated to manage local responsibilities and confidentiality within their work area.
Information Asset Owners	• Accountable to the SIRO for providing assurance on the security and use of the information assets within their respective area are identified, recorded and controls are in place to mitigate any risks.
Managers	• Ensure policy standards and guidelines are built into local processes to secure compliance • Ensure all job descriptions contain the relevant responsibility for information security, confidentiality and records managements • Ensure staff undertake IG mandatory training • Ensure any data protection incident is reported and investigated appropriately and escalated in the event of a serious incident.
Staff	• Must adhere to this Policy and all associated IG policies and procedures. • Mandated to undertake IG Training
3rd Party contractors	• Appropriate contracts that meet UK GDPR requirements to guarantee appropriate technical and organisational measures are in place that protect data subjects' rights for any service provider with potential or actual access to identified information assets.

Note: Under the UK GDPR WSBH is not required to appoint a Data Protection Officer as the type of organisation and scale of processing does not meet the definitions but is required to achieve its data protection obligations through sufficient staff and resources.

5. Definitions

Term	Definition
Caldicott Guardian	A senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically, and appropriately; to ensure that confidentiality is maintained.
Data Controller	An entity that decides how and why personal data is used e.g., the Hospice
Data Processor	An entity that processes data for and on behalf of the Data Controller
Data Protection Act 2018 (DPA)	Sets out the data protection framework for the UK and replaces the Data Protection Act 1998
Data Protection Impact Assessment (DPIA)	A process used within the Hospice to identify and minimise the data protection risks of a project
Data Protection Officer (DPO)	The UK GDPR requires that a DPO is appointed by a public authority or body and organisations carrying out certain types of processing activities
Data protection by design and by default	Implementation of the data protection principles to put in place the appropriate technical and organisational measures and to safeguard individual's rights
Data Security and Protection Toolkit (DSPT)	A mandatory annual assessment by NHS Digital which measures our performance against the National Data Guardian's ten data security standards
Data Subject	The identified or identifiable individual to whom the personal data relates.
Individual rights	There are eight rights for individuals, which have been strengthened in the UK GDPR. A data subject can ask WSBH to do something or stop doing something with their personal data
Lawful basis	The reason or legal grounds we rely on to use people's personal data. There are six bases to choose from (Appendix 4)
National Data Guardian	Advises and challenges the health and care system to ensure individual confidential information is safeguarded securely and used properly
Personal data	Any information, which directly or indirectly can identify an individual such as name, identification number or contact details

Term	Definition
Processing	Any action taken with someone's personal data e.g., collecting, recording, organising, sharing, erasure or destruction.
Pseudonymisation	The processing of personal data in a way that it cannot be attributed to a specific data subject without the use of additional information, provided that additional information is kept separate
Senior Information Risk Owner (SIRO)	An executive director or member of the board of directors with overall responsibility for an organisation's information risks
Special category data	Personal data which requires additional protections
UK GDPR	Is the retained version of the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales

6. Key Legislation

The DPA and the UK GDPR set out the legal requirements and duties placed on data controllers (the Hospice), and data processors (anyone the Hospice uses to process data on its behalf) and explains the 'information rights' held by data subjects (people we hold information about).

The policy will inform all staff how the UK GDPR applies to the Hospice and its obligations. Under the UK GDPR each controller of personal information must decide what the lawful basis is for processing personal information. If there is no relevant basis, then the processing is likely to be illegal and regulatory action could be taken against the Hospice.

7. Key Principles

7.1. UK GDPR principles

The UK GDPR has seven key principles which set out how the Hospice must process personal data, (see below). Compliance against the principles, is key and failure to comply may lead to regulatory action against the Hospice.

Principle	Description
Lawfulness, fairness, and transparency	Processing must be lawful and handled in a way which patients/staff/ supporters/customers would reasonably expect. The Hospice must be clear how personal data is processed.
Purpose limitation	The Hospice must be clear on the purpose of processing The Hospice needs to record the purpose of processing

Principle	Description
Data minimisation	Data must be adequate – sufficient to fulfil the purpose Relevant i.e., linked to the purpose Limited i.e., do not hold more than is required for the purpose
Accuracy	Staff should take reasonable steps to ensure personal data is not incorrect or factually misleading
Storage limitation	Personal data must not be kept longer than necessary for the purpose for which it was processed
Integrity and confidentiality (security)	The Hospice must ensure the appropriate technical and organisational measures are in place
Accountability	The Hospice is responsible for complying with the UK GDPR and must demonstrate its compliance

Each principle is detailed further in Appendix 3

7.2 Lawful basis for processing

The Hospice is obligated to have lawful basis to process personal data. There are six lawful bases for processing (Appendix 4). A lawful basis must be determined before processing begins.

The Hospice also processes special category information, which requires more protection. In order to lawfully process special category data the Hospice needs to identify a condition for processing, in addition to the lawful basis (Article 6 of the UK GDPR). This is known as an 'Article 9' condition (Appendix 4).

7.2.1 Consent

Consent may be given or withdrawn at any time. Where consent is relied upon as the condition for processing and it is then withdrawn, the Hospice must cease processing.

Consent is not an all-encompassing justification for processing personal data and does not obviate the Hospice's obligations with regard to the fairness, necessity and proportionality of data processing. For the avoidance of doubt, processing data may not be lawful even where consent has been given.

When seeking consent from patients, staff should also refer to the Hospice's Consent Policy CG03 and relevant professional guidance.
Where adult patients lack capacity to consent, decisions should be made in line with appropriate professional guidance and the Hospice's Assessing Capacity Policy CG06.

7.2.2 National Data Opt-Out

The national data opt-out enables patients to opt out from the use of their data for research or planning purposes in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients who object to their information being used for any purpose other than their own direct care must register with the National Data Opt-Out. Patients can view or change their national data opt-out choice at any time with the service.

The use of any patient data for any non-healthcare purpose, which is not also a legal requirement for the Hospice, must take account of the National Data Opt-Out.

The Hospice will ensure that where patients have exercised their rights to "opt out" of their information being used for secondary purposes, this will be respected.

7.3 Caldicott principles

The Caldicott principles focus on the protection and processing of patient identifiable information. These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals for both individual care and for other purposes.

The principles below are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and which they would reasonably expect to be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names, and addresses.

The Caldicott Principles	
Principle 1	Justify the purpose(s) of using confidential information
Principle 2	Only use it when absolutely necessary
Principle 3	Use the minimum that is required
Principle 4	Access should be on a strict need-to-know basis
Principle 5	Everyone must understand his or her responsibilities
Principle 6	Understand and 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

Full details of the principles can be found in Appendix 5.

7.4 Duty of confidentially

A duty of confidentiality is when one person discloses information to another, e.g. patient to clinician, in circumstances where it is reasonable to expect that information will be held in confidence.

It is:

- A legal obligation derived from case law
- A requirement established within professional codes of conduct
- Included in all WSBH staff members' contracts of employment.

Patients entrust staff with information about their health and treatment. They do so in confidence and have an expectation that staff will respect their privacy.

It is essential that the Hospice is seen to provide a confidential service to patients. Breaches of that confidentiality may lead to regulatory investigation and can result in disciplinary measures to those who have been negligent in causing the breach (see section 7.12).

7.5 Data Processing

Data processing covers the collecting, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintain confidence between the Hospice and its patients, staff, supporters and others with whom it operates.

The UK GDPR requires that processing of any personal information (healthcare and non-healthcare) held by the Hospice and has a lawful basis and satisfies one of the processing conditions.

Sharing of healthcare data for non-care reasons (often referred to as secondary purposes) will only take place where there is a lawful basis under Article 6 and Article 9. The Hospice will ensure data for any patients who have registered for the National Data Opt-Out service, see section 7.2.2, is not shared for this purpose.

7.6 IT systems

It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

The Information Security Policy (ICT001) provides detailed guidance on the security of Hospice IT systems including minimum standards of access controls.

Staff should not attempt to access or use electronic record systems that they have not been trained to use or authorised to access. Existing system users should not allow others to access systems using their login credentials.

Sharing system passwords is a disciplinary offence and viewed as a serious breach of Hospice procedure.

7.7 Communicating personal information

In order to provide effective care services, there is a need to transfer information between organisations and individuals. In order to comply with the UK GDPR principles, it is important that any transfer or communication of personal data is carried out securely and safely and that the risk of accidental disclosure or loss in transit is minimised.

Any data containing identifiable information that is transferred by the Hospice to an external party for processing must be securely encrypted during transit. Detailed guidance can be found in the Information Security Policy.

7.8 Access to information

7.8.1 Staff Access

Access to personal information is restricted and staff are prohibited from accessing or using patient information where there is no justification to do so.

While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

Staff have no right to access personal information held in records about their relatives or friends.

The Hospice's digital clinical systems will control access to any individual record held in that system. Users must only access individual personal records for those data subjects (patients, staff etc.) that they have authorisation to access for specific purposes.

The Hospice carries out audits of access to personal data and any member of staff who is found to be in breach of this guidance by inappropriately accessing their own or other people's records or personal data may face disciplinary action (see section 7.12).

In the case of unauthorised access to the Hospice's computer systems (including hacking and/or improper use of duly authorised credentials and the subsequent use of that data) may result in a criminal action under the terms Computer Misuse Act 1990.

7.8.2 Individual Rights

The UK GDPR provides enhanced rights for all individuals. These rights are mandated in the UK GDPR and the Hospice is required to act within a specific timeframe to any information request made to the Hospice.

There are eight rights of individuals which all Hospice employees and non-employees are required to follow (see Subject Access Policy IG07).

Information Right	Meaning
The right to be informed	Individuals have the right to be informed about how their data is used, which is included in the Hospice's privacy notice and patient information leaflet 'Your information, why we need your data and how is it used'
The right of access (Subject Access request)	Individuals have the right ask for and receive a copy of their personal data
The right to rectification	Individuals have the right to have inaccurate personal data rectified or completed if incomplete
The right to erasure (Right to be forgotten)	Individuals have the right to ask for information to be erased; this is not an absolute right and only applies in certain circumstances
The right to restrict processing	Individuals have the right to request the restriction or suppression of their personal data; this is not an absolute right and only applies in certain circumstances.
The right to data portability	Allows individuals to obtain and reuse their personal data for their own purposes
The right to object	Individuals have the right to object to the processing of their personal data in certain circumstances
Rights in relation to automated decision-making	Where there is no human involvement in decision-making or profiling, this is restricted and can be challenged

7.9 Data protection by design and by default

As part of the UK GDPR's accountability principle, the Hospice is required to safeguard individual rights by putting in place the appropriate technical and organisational measures.

The UK GDPR requires the Hospice to integrate data protection into every aspect of processing activity. This includes implementation of the data protection principles and the safeguarding of individual rights, such as data minimisation, pseudonymisation and purpose limitation as set in this policy.

The Hospice requires that data protection must be considered at the start of any new project, service, or process, see section 7.10.

7.10 Data Protection Impact Assessment (DPIA)

A DPIA identifies and assesses potential risks to the Hospice of processing activities. It is an integral part of data protection by design and by default and it should be completed for all projects, proposals or business changes that involve personal information.

Staff involved in procurements of new systems, the setting up of new services or ways of working are responsible for ensuring that the IG Lead is involved in the project plan and that a DPIA is completed.

7.11 Data sharing – third parties

Where the Hospice (as Data Controller) shares healthcare data for non-care reasons with another organisation, a data sharing agreement must be put in place.

For all other non-healthcare personal data, that the Hospice instructs a third-party organisation to process on their behalf, a contract must be in place which confirms the responsibilities of each party and the appropriate technical and organisational measures in place to ensure that the processing complies with the UK GDPR and protects the rights of individuals.

7.12 Breach of data protection and confidentiality

Any breach or suspected breach of data protection and confidentiality can have severe implications for the Hospice, its patients, staff and supporters.

The WSBH Notification of Data Security and Protection Incidents Policy (IG08) sets out the process for all data incidents or near misses to be recorded on the Hospice's Incident reporting system (Sentinel). This provides the mechanism for incidents to be monitored, managed, investigated and for lessons to be learned.
The Governance Committee (quarterly) receives reports on incidents, complaints and near misses. Under data protection legislation, serious incidents must be reported to the ICO within 72 hours. The ICO regulates and enforces data protection law and can fine an organisation that has not complied with data protection legislation. All serious incidents will be reported to the Management Team and Board by exception.

Breaches of confidentiality or unauthorised disclosure of any information subject to the DPA and UK GDPR constitutes a serious disciplinary offence or gross misconduct under the Hospice's Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

7.13 Disposal of personal information

It is a principle of the UK GDPR that data should 'not be kept for longer than necessary'. Records will be stored securely for the appropriate length of time in accordance with the Records Management Code of Practice 2021 (a guide to the management of health and care

records) for clinical records and the Corporate Records Retention and Disposal Schedule for non-clinical records.

All printed information, reports and printed copies of records containing personal data should be kept securely at all times; this includes but is not limited to handover reports and documents used by staff working on the Inpatient Unit (IPU).

Any documents containing personal data should be disposed of securely and not discarded in general waste or recycling bins. The Hospice commissions a confidential waste disposal service and provides regular collections of confidential waste from all Hospice areas.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops, and any other devices with information storage capabilities) should be carried out through the IT Department to ensure that all data is effectively removed before disposal.

8. Advice and Guidance

The IG Lead and Caldicott Guardian will provide subject matter advice when required.

9. Communication and Training

A needs analysis will be undertaken on an annual basis to identify training required by all staff including those with identified key roles.

The Data Protection and Confidentiality Policy will be uploaded to the mandatory training system (Blue Stream Academy, BSA), and made available on the Resources Drive. Awareness will be cascaded through governance and team meetings.

All staff are required to undertake mandatory training using the Hospice e-learning system (BSA) or through the provision of evidence of completed external training. This requirement applies to agency staff and contractors working at the Hospice who may have access to personal information.

Mandatory IG training for all staff is included in the Hospice's statutory and mandatory training requirements. Training compliance is monitored and reported to the Governance Committee.

10. Monitoring Compliance

The purpose of monitoring is to provide assurance that the agreed approach is being followed. Monitoring will be proportionate, achievable and deal with specifics that can be assessed or measured, see table below.

Measurable policy objective	Monitoring Method	Monitoring Frequency	Responsible Person	Responsible Committee
DSP Self-Assessment	DSP toolkit	Annual	SIRO	Governance Committee
Data protection & confidentiality incidents	Sentinel	Monthly	IG Lead	Governance Committee
Personal data breaches reported to the ICO	Sentinel	Immediate escalation	IG Lead	Management Team
Induction and annual mandatory IG training compliance levels	Governance Report	Monthly	Education and Training Manager	Governance Committee
Data protection by design and by default	DPIA assessments	Annual	IG Lead	Governance Committee
Policy Compliance	Data Security and Protection Audit	Annual and in response to a serious incident or trend.	Quality Assurance Manager	Governance Committee

Compliance with this policy will be monitored via the Governance Committee.

This policy will be reviewed three yearly or more frequently in accordance with legislation or national guidance changes.

11. Equality Impact Assessment

WSBH is committed to creating a positive culture for all staff and service users.

The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment, pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

PROTECTED CHARACTERISTIC	EQUALITY IMPACT ASSESSMENT
Age	There is no evidence to indicate that any staff member or volunteer represented in these Protected Characteristic groups is, as a result of this Policy, affected more or less favourably than staff and volunteers in other groups
Sex	
Gender Re-assignment	
Sexual Orientation	
Race	
Religion or Belief	
Marriage / Civil Partnership	
Pregnancy / Maternity	
Disability	

12. References

- Data Protection Act (2018)
- UK General Data Protection Regulation
- Common Law Duty of Confidentiality
- National Health Service Act (2006)
- Health and Social Care Act (2012)
- The Health and Social Care (Safety and Quality) Act (2015)
- Health and Social Care (National Data Guardian) Act (2018)
- Access to Health Records Act (1990)
- Human Rights Act (1998)
- Information Commissioner's Office website: https://ico.org.uk/
- The Eight Caldicott Principles 2020, https://www.gov.uk/government/publications/the-caldicott-principles, and associated guidance from the National Data Guardian https://www.gov.uk/government/organisations/national-data-guardian
- Department of Health Confidentiality: NHS Code of Practice (November 2003): https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- Computer Misuse Act (1990

13. Appendices

Appendix 1: Data Security Standards

Appendix 2: Relevant WSBH Information Governance Policies

Appendix 3: UK GDPR Principles

Appendix 4: UK GDPR – Lawful bases, conditions, and special category data

Appendix 5: Caldicott Principles

Appendix 1

The 10 Data Security Standards

People	Process	Technology
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.	**Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.**	**Ensure technology is secure and up to date.**
1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.	4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals.	8. No unsupported operating systems, software or internet browsers are used within the IT estate.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to to handle information responsibly and their personal accountability for deliberate or avoidable breaches.	5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.	9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit	6. Cyber attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.	10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.
	7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.	

Appendix 2: Relevant WSBH Information Governance Policies

- ICT001 Information Security Policy
- ICT002 Mobile and Remote Access Policy
- IG01 Information Governance Policy
- IG03 Data Quality Policy
- IG04 Clinical Records Management
- IG05 Organisational Change Policy
- IG06 Data Impact Assessment Policy
- IG07 Subject Access Requests Framework
- IG08 Notification of Data Security and Protection Incidents Policy

Appendix 3: UK GDPR Principles

The UK GDPR sets out seven key principles with which the Hospice is required to comply	
Article 5(1)(a) Lawfulness, fairness and transparency	Personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')
Article 5(1)(b) Purpose limitation	Personal data shall be: 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
Article 5(1)(c) Data minimisation	Personal data shall be: c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
Article 5(1)(d) Accuracy	Personal data shall be: 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 ('accuracy')
Article 5(1)(e) Storage limitation	Personal data shall be: 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 ('storage limitation')
Article 5(1)(f) Integrity and confidentiality (security)	Personal data shall be: 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
Article 5(2) Accountability	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Appendix 4: UK GDPR – Lawful bases, conditions, and special category data

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever the Hospice processes personal data	
Article 6(1)(a) Consent	The individual has given clear consent for you to process their personal data for a specific purpose
Article 6(1)(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
Article 6(1)(c) Legal obligation	The processing is necessary for you to comply with the law (not including contractual obligations)
Article 6(1)(d) Vital interests	The processing is necessary to protect someone's life
Article 6(1)(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
Article 6(1)(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.)

Special Categories of Personal Data
The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection: • Personal data revealing racial or ethnic origin; • Personal data revealing political opinions; • Personal data revealing religious or philosophical beliefs; • Personal data revealing trade union membership; • Genetic data; • Biometric data (where used for identification purposes); • Data concerning health; • Data concerning a person's sex life; and • Data concerning a person's sexual orientation.

If special category data is processed one of the following condition(s) must also be met. Article 9 lists the conditions for processing special category data	
Article 9(2)(a) Explicit consent	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law prohibits processing by the data subject

Article 9(2)(b) **Employment, social security and social protection (if authorised by law)**	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 domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject
Article 9(2)(c) **Vital interests**	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
Article 9(2)(d) **Not-for-profit bodies**	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 disclose without the consent of the data subjects
Article 9(2)(e) **Made public by the data subject**	processing relates to personal data which are manifestly made public by the data subject
Article 9(2)(f) **Legal claims or judicial acts**	processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial
Article 9(2)(g) **Reasons of substantial public interest (with a basis in law)**	processing is necessary for reasons of substantial public interest, on the basis of domestic 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
Article 9(2)(h) **Health or social care (with a basis in law)**	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 domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (processed by or on behalf of a professional subject to professional secrecy obligation)

Article 9(2)(i) Public health (with a basis in law)	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 domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
Article 9(2 (j) Archiving, research and statistics (with a basis in law)	processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the DPA) based on domestic 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 5

The Eight Caldicott Principles

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

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

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.