Data Security and Protection Policy	
Post holder responsible for Procedural/Policy Document	Head of Governance and Data Protection
Policy Guardian/Author	Head of Governance and Data Protection
Department responsible for Procedural Document	Governance
Contact details	01392 688099 Dpo.hospiscare@nhs.net
Date of original document	12th March 2019
Impact Screening performed	**Yes**
Ratifying body and date ratified	Senior Management Team – 12th March 2019
Review date (and frequency of further reviews)	*2 years – March 2023*
Expiry date	*June 2023*
Date document becomes live	16th June 2021
Dissemination plans	Via Staff comms and on the Intranet and Internet

Please *specify* standard/criterion numbers and tick ✓ other boxes as appropriate

Monitoring Information		Evidence Provided	
Patient Experience			
Safety			
Assurance Framework	✓		
Monitor/Finance/Performance			
CQC Regulations/Outcomes	✓		
Other (please specify):	✓	Data Protection Legislation Data Security and Protection toolkit	✓
Strategic Plans and Roadmaps			
Note: This document has been assessed for any equality, diversity or human rights implications ✓			

Controlled document
This document has been created following the Hospiscare policy on procedural documents. It should not be altered in any way without the express permission of the author or their representative.

Full History		**Status: Final**	
Version	Date	Author	Reason
1.0	Feb 2015	Director of Finance and ICT	Creation of Policy
2.0	12th March 2019	Governance Officer	Review and Update of Policy in line with GDPR
3.0	26th April 2021	Head of Governance and Data Protection	Rewrite of current policy to update and include toolkit requirements
3.1	15th June 2021	Head of Governance and Data Protection	Signed off at SMT

Associated Trust Policies/ Procedural documents:	Information Governance Policy Information, Communications and Technology User Policy (ICT) Mobile Computing and Working from Home Po Incident Policy Clinical Record Keeping Policy
Legislative Requirement/ Best Practice reference	Data Protection Act 2018 General Data Protection Regulation 2016 Health and Social Care Act 2012 Equality Act 2010
Key Words:	Data, Personal, Special, Legal basis
In consultation with and date: Information Governance Group Senior Management Team	
Contact for Review:	Kelly Prince
Executive Lead/Board Chair Signature:	Andrew Randall - CEO

DATA SECURITY AND PROTECTION

POLICY

1. Reason(s) for the policy

Best practice ✓
Legal compliance ✓
Regulatory compliance ✓
Good governance✓
Risk mitigation ✓

The purpose of this Data Protection Policy is to outline the principles and obligations of the Data Protection Act 2018, the General Data Protection Regulation 2016, The 10 National Data Guardian Security Standards, the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

2. Policy Statement

2.1 Hospiscare's vision is to ensure that those in need receive outstanding end of life care, in the place of their choice

Our mission – To provide compassionate, expert end of life care to those in need – before, during and after death. Together with our local community, we make everyday matter

We aim to provide the best possible service in line with our values

- ✓ Compassionate
- ✓ Respectful
- ✓ Professional
- ✓ Inclusive

2.2 Introduction

Hospiscare has a legal obligation to comply with the provisions of the Data Protection Act 2018 & GDPR 2016; the key pieces of legislation covering security and confidentiality of personal information. All legislation relevant to an individual's right to confidentiality and the ways in which that can be achieved and maintained are paramount to the organisation.

The aim of this policy is to enable the organisation to comply with the law. To do this it needs to keep certain information about its staff, supporters and patients secure and confidential. Information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2.3 Purpose

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers

Our data protection principles and commitment to common law and legislative compliance;

The procedures for data protection by design and by default.

To achieve this, the organisation will follow the Principles set out below.

2.4 Data Protection Principles

The 7 Data Protection Principles outlined in the DPA 18 state how the organisation must process personal data. Appendix 1 describes Personal and Special Category Data.

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and kept up to date;
- 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 ('storage limitation');
- Processed in a manner that ensures appropriate security of the personal data; - Integrity and Confidentiality
- Accountability – The controller shall be responsible for, and be able to demonstrate compliance with the Principles

2.5 – Individual Rights

We uphold the personal data rights outlined in the GDPR;

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;

- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

2.6 – Data Protection Officer

In line with required legislation we employ a Data Protection Officer (DPO) who reports to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

Main outline of the Data Protection Officer Role

The DPO is responsible for overseeing an organisation's data protection strategy and implementation. They are the officer that ensures that an organization is complying with the GDPR's requirements. According to **GDPR Article 39** a data protection officer's responsibilities include:

- Training organisation employees on GDPR compliance requirements
- Conducting regular assessment and audits to ensure GDPR compliance
- Serving as the point of contact between the company and the relevant supervisory authority
- Maintaining records of all data processing activities conducted by the company
- Responding to data subjects to inform them about how their personal data is being used and what measures the company has put in place to protect their data
- Ensuring that data subjects' requests to see copies of their personal data or to have their person data erased are fulfilled or responded to, as necessary.

2.7 Data protection by design & by default

2.7.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

2.7.2 We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

2.7.3 Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) and if it is decided that one is appropriate, the Hospiscare process for completion of this assessment will be undertaken

2.7.4 All new systems used for data processing will have data protection built in from the beginning of the system change.

2.7.5 All existing data processing has been recorded on our Information Asset register which include Register of Processing Activities (ROPA).

2.7.6. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

2.7.7. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

2.7.8 Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

3. Scope

This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

This policy applies to all staff, volunteers and contractors/third parties.

4. Responsibilities

The Board of Trustees delegates responsibility for implementing this policy to the Head of Governance and Data Protection (DPO). The Data Protection Officer and Information Governance Group (IGG) will support the Board in identifying and monitoring the data protection issues that the charity is exposed to.

Senior Information Risk Owner (SIRO) The organisations identified SIRO is responsible for implementing an effective but proportionate framework to enable the charity to meet its obligations on protecting data. The SIRO also ensures information security incidents and risks, together with the required remedial actions, are reported to the relevant bodies. The SIRO will brief the Board of Trustees on all data protection issues.

The Head of Governance and Data Protection is the organisation's Data Protection Officer (DPO). If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to the DPO.

Hospiscare has a nominated Caldicott Guardian (CG) who assesses and deals with breaches and issues of a clinical nature. They are regarded as the conscience of the organisation. They will make decisions about what is appropriate when our normal policies cannot be applied.

The Head of Governance and Data Protection is responsible for the completion of the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT and to be the point of contact for Subject Access Requests.

The Information Asset Owners (IAO) will be a senior member of staff who is responsible for information assets within their department. It is a core IG objective that all Information Assets of the hospice are identified and that the business importance of those assets is established. Details can be found on the Information Asset Register.

Staff and volunteers are responsible for reporting data protection/security issues they become aware of and supporting managers in managing risks. Staff and volunteers are responsible for keeping confidential data secure and for ensuring they comply with this requirement on a day to day basis.

All staff must complete Annual Data Security and Protection e-learning training

5. Equality Impact Assessment

This can be found at Appendix 4

Appendix 1 – Personal and Special Category Data

Personal data

The Data Protection Act 2018 applies to personal data that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it. Information is "personal data" if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

Consequently, automated and computerised personal information about employees, supporters or patients held by Hospiscare is covered by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.
A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each employee filed in date order, i.e. a system to guide a searcher to where specific information about a named employee can be located easily.

Special Category Data

Special category data (previously sensitive personal data) is information about an individual's:

- race
- political opinions
- religious beliefs
- trade union membership
- genetics & biometrics
- health
- sex
- Art. 10 Criminal records data

The organisation will process special category data, including sickness and injury records and references, in accordance with the six data protection principles. If the organisation enters into discussions about a merger or acquisition with a third party, the organisation will seek to protect employees' data in accordance with the data protection principles.

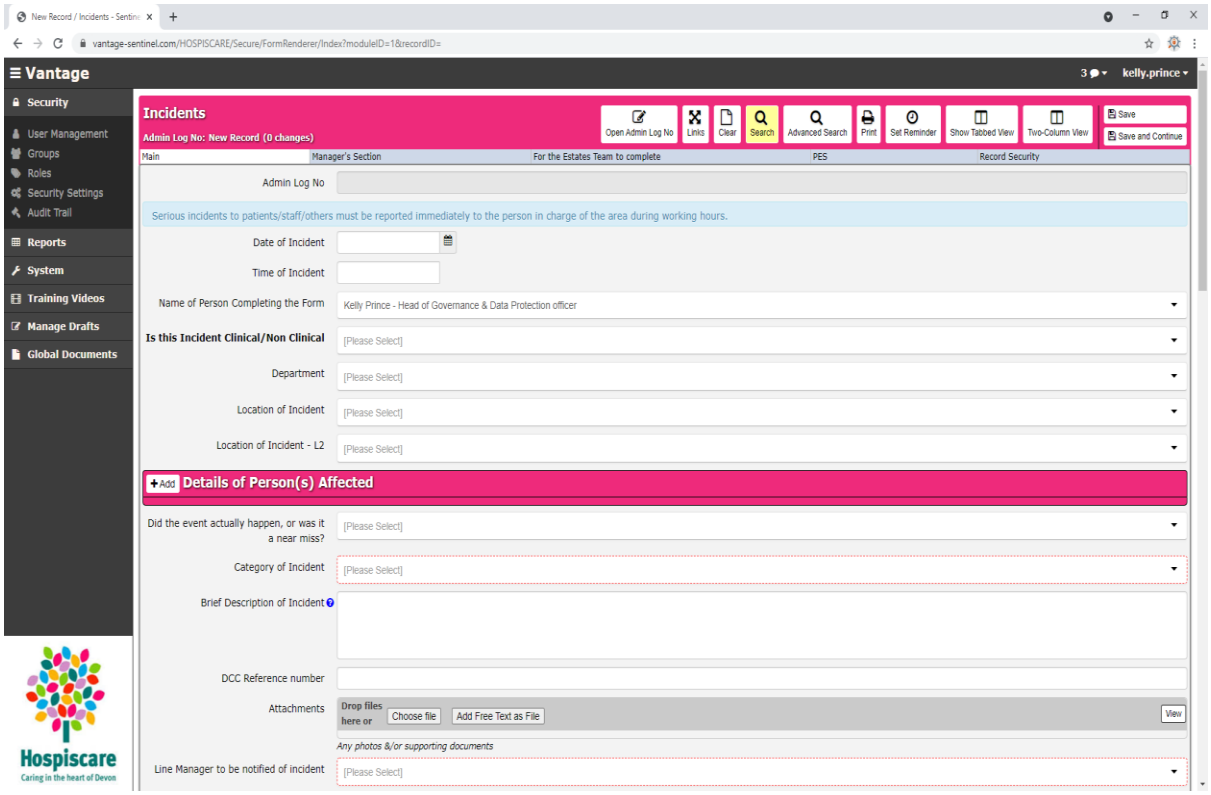
Appendix 2 – Data Breach Incident Reporting Process

The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. Hospiscare must report any of these breaches 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, Hospiscare must also inform those individuals without undue delay.

Hospiscare has a robust method of breach protection. All Clinical and non-clinical breaches must be reported on the Vantage Incident management module

All breaches reported raise an alert to the Data Protection Officer and Caldicott Guardian. You must complete the form as fully as possible.



Appendix 3 – Information and Cyber Security

A key principle of the UK GDPR is that Hospiscare process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

Data must be stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.

The UK GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

This reflects both the UK GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.

To ensure compliance you are required to consider things like risk analysis, organisational policies, and physical and technical measures.

Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.

The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

The National Cyber Security Centre (NCSC) has tools and resources to help you to develop an approach that you can use when assessing the measures that will be appropriate for you.

Hospiscare has an IT Security policy that outlines these requirements further.

Appendix 4 – Equality Impact Assessment Tool

Name of document	**Data Protection Policy**
Department	Head of Governance and Data Protection
Name, job title and contact details of person completing the assessment	Kelly Prince Head of Governance and Data Protection
Date completed:	**10th May 2021**

The purpose of this tool is to:

- **Identify** the equality issues related to a policy, procedure or strategy
- **Summarise the work done** during the development of the document to reduce negative impacts or to maximise benefit
- **Highlight unresolved issues** with the policy/procedure/strategy which cannot be removed but which will be monitored, and set out how this will be done.

1. What is the main purpose of this document?

This document sets out the rights and responsibilities that must be undertaken by Hospiscare in order to conform to the Data Protection Act 2018 and associated legislation

2. Who does it mainly affect? *(Please insert an "x" as appropriate:)*

Volunteers X Staff X Patients X Other (please specify) ☐

3. Who might the policy have a 'differential' effect on, considering the "protected characteristics" below? (By *differential* we mean, for example that a policy may have a noticeably more positive or negative impact on a particular group e.g. it may be more beneficial for women than for men)

Please insert an "x" in the appropriate box *(x)*

Protected characteristic	**Relevant**	**Not relevant**
Age	☐	☐
Disability	☐	☐
Sex - including: Transgender, and Pregnancy / Maternity	☐	☐
Race	☐	☐

Religion / belief	☐	☐
Sexual orientation – including: Marriage / Civil Partnership	☐	☐

4. **Apart from those with protected characteristics, which other groups in society might this document be particularly relevant to** *(e.g. those affected by homelessness, bariatric patients, end of life patients, those with carers etc.)*?

None

5. **Do you think the document meets our human rights obligations?** ☒

Feel free to expand on any human rights considerations in question 6 below.

A quick guide to human rights:
• ***Fairness –*** *how have you made sure it treat everyone justly?* • ***Respect –*** *how have you made sure it respects everyone as a person?* • ***Equality –*** *how does it give everyone an equal chance to get whatever it is offering?* • ***Dignity –*** *have you made sure it treats everyone with dignity?* • ***Autonomy –*** *Does it enable people to make decisions for themselves?*

6. **Looking back at questions 3, 4 and 5, can you summarise what has been done during the production of this document and your consultation process to support our equality / human rights / inclusion commitments?**

Please give a brief summary- identifying: Al relevant areas have been explored and varying rights taken into account.

7. **If you have noted any 'missed opportunities', or perhaps noted that there remains some concern about a potentially negative impact** please note this below and how this will be monitored/addressed.

"Protected characteristic":	N/A
Issue:	
How is this going to be monitored/ addressed in the future:	
Group that will be responsible for ensuring this carried out:	