Data Protection Policy

Title:	Data Protection
Procedural document Type:	Policy
Reference:	IG004
Version:	Six
Approved and Ratified by:	Finance Committee
Date Approved and Ratified:	28 February 2023
Name of responsible team:	Information Governance
Review Frequency:	Three years
Review Date:	28 February 2026
Target Audience:	All Staff

Contents

Please Note the Intention of this Document

Cornwall Hospice Care needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), volunteers, donors, suppliers and other business contacts. The information includes name, address, email address, data of birth, private and confidential information, sensitive information. In addition, we may occasionally be required to collect and use this information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with the current Data Protection Act 2018 (the Act) and the UK GDPR.

This document sets out and describes the way in which this compliance shall be achieved.

Review and Amendment Log

Version No	Type of Change	Date	Description of change
One	Creation		
Three	Amended	June 2017	Adapted for GDPR.
Four	Planned Review	November 2018	
Five	Update	June 2022	Updated and reformatted.
Six	Update	February 2023	Updated and reformatted.

1. Scope

This policy is to be applied to Cornwall Hospice Care Ltd., Cornwall Hospice Care Lottery Ltd. and Cornwall Hospice Care Trading Ltd. known collectively in this policy as Cornwall Hospice Care (CHC) or the Charity.

However, as separate legal entities each has its own Data Protection Registration with the Information Commissioners Office (ICO)

This policy applies to all staff and volunteers working for the Charity (paid or unpaid) this includes bank staff, contractors and students on placements etc. irrespective of geographical location and role.

2. Introduction

The Charity needs to collect and use certain types of information about the Data Subjects (people whose data is collected) in order to carry on its work. Personal information must be collected and dealt with appropriately – whether on paper, in a computer or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 2018 and UK GDPR.

3. General Data Protection Regulation (GDPR)

The European General Data Protection Regulations (GDPR) became mandatory with effect from 25 May 2018 along with the Data Protection Act 2018 (DPA). This policy is based on the requirements of the GDPR and the DPA.

When the UK left the EU the GDPR was retained as the 'UK GDPR'.

The UK GDPR principles should be read in conjunction with the DPA (1998), which has additional detail at certain points and a new **accountability** requirement. The UK GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed in separate articles (GDPR Chapter III and Chapter V respectively).

The most significant addition is the accountability principle. The UK GDPR requires organisations to show **how** they comply with the principles – for example by documenting the decisions taken about a processing activity.

Organisations may be fined for not complying with the UK GDPR irrespective of whether that has been an information breach or not. Fines under the GDPR have increased from a maximum of £500,000 (under the DPA 1998) to a maximum of the greater of 20 million Euros or 4% of global turnover under UK GDPR.

The UK GDPR makes completion of Privacy Impact Assessments an explicit requirement of data protection law and has updated and renamed them Data Protection Impact Assessments (DPIAs). Good guidance on how to undertake these is available from the ICO who have prepared a document "Conducting privacy impact assessments code of practice". It remains best practice to consider these issues at the start of the development work on any new systems or workflow that may involve personal information.

Addressing these points early in the process normally yields a better, more cost-effective solution, which is more likely to achieve UK GDPR compliance.

4. Terms and Definitions

The following is a list of definitions of the technical terms used and is intended to aid understanding of this policy.

Data Controller – The organisation that determines the purposes for which and the manner in which any personal data are or are to be processed. CHC is the Data Controller under the Data Protection Act 2018, and UK GDPR, and determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for (i.e. complete an ICO registration).

Data Protection Act 2018 (DPA) – The current UK legislation that provides a framework for responsible behaviour by those using personal information, this should be used in conjunction with the UK GDPR.

Data Protection Officer (DPO) – The CHC DPO is the Finance Director.

Data Subject – The individual who is the subject of personal data.

'Consent' and 'Explicit consent' – is a freely given, specific, unambiguous and informed agreement by a Data Subject to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data. Under UK GDPR there is little practical difference between consent and explicit consent.

* See 'Informed Consent' definition below

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018 and UK GDPR as the UK 'Supervising Authority'.

Processing – means collecting, amending, using, handling, storing, viewing or disclosing information.

Personal Information – any information, held in any format relating to a living individual who can be identified either from the data or from the data in conjunction with other information that is in, or likely to come into, the possession of the data controller. This includes employment details, patient and client information, donor and supporter information, customer information and information captured on CCTV. Note that under UK GDPR items such as IP addresses, email addresses and other information that is, or can be, unique to an individual may also be considered to be personal data.

Sensitive data – means data about:

- Racial or ethnic origin.
- Political opinions.
- Religious or similar beliefs.
- Trade union membership.
- Physical or mental health.
- Sexual life.
- Criminal record.
- Criminal proceedings relating to a data subject's offences.

Informed Consent is when:

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data, and
- Then gives their consent.

5. Duties

Chief Executive is responsible for:

Ensuring adequate resources are in place for the implementation of this policy and delegate day to day responsibility for this to the Data Protection Officer, Senior Information Risk Owner (SIRO) and the Caldicott Guardian.

Data Protection Officer (DPO) is responsible for:

- Informing and advising the Charity and its employees about their obligations to comply with the DPA/UK GDPR and other data protection laws.

- Monitoring compliance with the DPA/UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Being the first point of contact for supervisory authorities (ICO) and for individuals whose data is processed.

The CHC Finance Director is the DPO.

Caldicott Guardian is responsible for:

- Providing advice and guidance in the use and sharing of patient (service user) information i.e. the application of the Caldicott Guardian Principles (see Appendix 1).
- Approving, monitoring and reviewing protocols governing access to service user identifiable information by staff within the Hospices and by relevant other agencies.
- Overseeing the control of access to and disclosure of healthcare records.

The CHC Director of Clinical Services is the Caldicott Guardian.

Senior Information Risk Owner (SIRO) is responsible for:

Ensuring the organisation's information risks are identified and managed, and that appropriate assurance mechanisms exist. The CHC Finance Director is the SIRO.

Information Governance Officer is responsible for:

- Implementing the Information Governance work program across the Charity.
- Monitoring actual or potential reported information security incidents within the organisation.
- Ensuring the effectiveness of the Information Governance (IG) incident reporting system and procedures.

Information Asset Owners are responsible for:

Managing/maintaining the security and integrity of the information assets assigned to them.

Senior Managers and Managers are responsible for:

- Ensuring that the policy and its supporting procedures and standards are built into local processes and that there is ongoing compliance.

- Ensuring that all staff job descriptions contain relevant responsibility for personal information security, confidentiality and records management.
- Ensuring their staff undertake information governance training.
- The security of the physical environment where their team operates and where information is processed and stored.
- Ensuring that all sources of person identifiable information sent into or out of the Charity are advised of the requirements of this policy.
- Reporting and investigating any breaches of this policy.

The ICT Manager is responsible for ensuring all computer hardware and software is safeguarded in line with the DPA/UK GDPR and provide relevant reports to the appropriate person (SIRO, DPO, Information Governance Forum) to assist with monitoring compliance or incident investigations.

All staff and volunteers are responsible for:

- Complying with this policy and its supporting procedures, including maintenance of data confidentiality and data integrity.
- Maintaining the operational security of the information systems they use.
- Ensuring they complete any training as required.
- Reporting any breaches of this policy through the information incident reporting process (Appendix 4).
- Checking that personal data held on themselves is accurate and up to date and updating the Human Resources Team accordingly of any changes (e.g. change of address).

6. Data Sharing

CHC may share data with other agencies such as the NHS, local authority, funding bodies, Department of Work and Pensions and other Government and voluntary agencies (see Annex A).

UK GDPR also permits the sharing of patient information between clinicians for the purpose of the direct care of that patient. This means, for example, that a Hospice clinician may share information about a patient with that patient's GP.

The Data Subject will be made aware, in most circumstances, of how and with whom their information will be shared and in line with the rights of data subjects the wishes of data subjects regarding the sharing and use of their data will where possible be implemented.

Where third parties are used in the processing or storage of data then Data Protection requirements of the UK GDPR are included within contracts, data sharing agreements or through individual Non-Disclosure Agreements (NDA).

There are circumstances where the law allows the CHC to disclose data (including sensitive data) without the data subject's consent.

These are when:

a) Carrying out a legal duty or as authorised by the Secretary of State.
b) Protecting vital interests of a Data Subject or other person.
c) The Data Subject has already made the information public.
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
e) Monitoring for equal opportunities purposes – i.e. race, disability or religion.
f) Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

CHC regards the lawful and correct treatment of personal information as essential to successful working, and to maintaining the confidence of those with whom we deal.

7. Principles of Data Protection

CHC will adhere to the following data protection principles:

Personal and sensitive data shall be:

- Processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met (i.e. the conditions of the DPA and UK GDPR).
- Obtained only for one or more of the purposes specified in the DPA/GDPR, and shall not be processed in any manner incompatible with that purpose or those purposes.
- Adequate, relevant and not excessive in relation to those purpose(s).
- Accurate and, where necessary, kept up to date.
- Processed in accordance with the rights of data subjects under the Act/UK GDPR,
- Kept secure and the Data Controller will take appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information, and personal and sensitive data.
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of

protection for the rights and freedoms of data subjects in relation to the processing of personal information.
- Shall not be kept for longer than is necessary

The CHC will, through appropriate management, strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Ensure that the rights of people about whom information is held, can be fully exercised under the DPA and UK GDPR.

  These include:

  - ❖ The right to change or remove their consent for processing their personal data.
  - ❖ The right to be informed that processing is being undertaken,
  - ❖ The right of access to one's personal information
  - ❖ The right to prevent processing in certain circumstances
  - ❖ The right to correct, rectify, block or erase information, which is regarded as wrong information.
  - ❖ The right to be 'forgotten' (see Appendix 3).

- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information.

8. Data Access (Subject Access Requests)

All Data Subjects have the right to access the information CHC holds about them (i.e. make a subject access request (SAR)) and the CHC will comply with the ICO "Subject access code of practice" in dealing with these requests. However it should be noted that the GDPR has changed some aspects of this code –

specifically that the time to respond has reduced from 40 days to one month (we use 28 days) and that it is no longer permitted to make a charge for completing a subject access request.

Information provided for a SAR must have the Data Subject as its focus, not merely mentioned in passing. Records may be redacted to remove details of third parties (but not those of relevant health professionals).

A member of staff, volunteer or other Data Subject, may make a written request to access the information held about them by application to the Chief Executive Officer (CEO), the Director of Clinical Services, the Finance Director or a Clinician, manager or the Human Resources team.

Staff information held generally for the purposes of management planning or forecasting are exempt from SAR information provision above.

A SAR received in any part of the CHC should be passed to the Data Protection Officer for registering and processing.

Full details of the CHC SAR process can be found in the 'CHC Access to Health Records policy and procedure'.

9. Data Collection

The document **'Your Information - Privacy Matters at Cornwall Hospice Care'** at Annex A gives an overview of the legal basis and reasons for data collection by the Charity.

9.1 Obtaining Consent

In areas where 'Consent' is the legal basis for data processing CHC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data with consent, CHC will ensure that the Data Subject:

- Clearly understands why the information is needed.
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing.
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.

- Has received unambiguous and sufficient information on why their data is needed and how it will be used.

Also see Appendix 2 – 'ICO Guidance on how to obtain, record and manage consent'.

9.2 Managing Data Subjects Contact Preferences

Data subjects have the right to change their minds regarding consent to collect or share personal or sensitive information at any time. When using consent as the legal basis for collecting or sharing information the Charity will keep records where consent has or has not been agreed and amend these records at the request of verified data subjects.

In addition, irrespective of the legal basis for collecting/using information the Charity will, where practicable, cease contacting data subjects upon their request e.g. stop sending marketing material on request.

The Charity will at all times comply with Mail and Telephone Preference Services registrations and not market to those requesting no contact by direct mail or telephone.

9.3 Data Storage

Personal and/or sensitive information and records relating to data subjects will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed for the purpose that it was collected or required by statute and will be disposed of appropriately i.e. paper records will be disposed of using the CHC process for disposing of confidential waste. Electronic records will be destroyed as per the ICT Security Policy. In both cases records will be maintained in line with the CHC Records Retention policy (see the 'Management, Storage and Destruction of Health Records Policy' that contains the CHC data retention schedules).

It is CHC's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

9.4 Data Accuracy

The CHC will also take steps ensure that this information is kept up to date e.g. by routinely or periodically asking data subjects whether there have been any changes to their data.

In addition**,** the CHC will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they are responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised.
- Anybody wanting to make enquiries about handling personal information knows what to do i.e. discuss with line management who will be supported by the DPO.
- It deals promptly and courteously with any enquiries about handling personal information.
- It describes clearly how it handles personal information – through Privacy and Fair Processing notices.
- It will regularly review and audit the ways it holds, manages and uses personal information. It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them**.**

10. Information Incident Reporting

In the event of a suspected information security or confidentiality breach occurring the following process should be followed:

All incidents, suspected incidents and near misses should be reported as soon as practically possible (normally within 24 hrs).

The UK GDPR requirement is for serious incidents to be reported to the ICO within 72 hours of confirmation of the incident occurring.

- The person discovering an actual or suspected information breach or incident should report it to their line manager (this includes near misses).

- The line manager should ensure action is taken to contain the incident/prevent a recurrence.
- The incident should be reported to the area's Executive management.
- An Information Incident Report form (Appendix 4) should be completed and sent to the Information Governance (IG) Officer (rward@cornwallhospice.c.uk).
- IG will carry out an assessment and determine, in conjunction with management, what investigation is needed.
- Who should carry it out?
- Who should receive the report?
- The IG Officer will ensure the Caldicott Guardian is made aware of the incident.
- All reported IG incidents are logged onto the NHS Incident Reporting system.
- Reported through the IG Forum.

The Information Incident reporting form is located in Appendix 4 and on the Information Governance/Public IG Library folder on the CHC Intranet (Office 365) or may be obtained by contacting the IG Officer by email or on 01726 66868 Option 7.

The NHS 'Guide to the Notification of Data Security and Protection Incidents' and incident reporting tool are used to assist in determining the severity of incidents and manage the appropriate external reporting of them, i.e. to the ICO in the case of a serious incident.

11. Retention of Records

UK GDPR and the DPA states that data should not be kept for any longer than necessary for the purpose for which they were obtained. The record retention schedule for CHC is contained within the 'CHC Management, Storage and Destruction of Health Records Policy'.

12. General

Failure to adequately comply with the content and principles of this policy may lead to staff/volunteer disciplinary action and/or monetary penalties by the ICO against the individual or the Charity.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the DPA/UK GDPR.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer (Finance Director).

12.1 Implementation and Dissemination

Once ratified this policy will be loaded to the intranet and replace the current Data Protection Policy.

12.2 Training and Support

Formal Information Governance training is provided within CHC induction and mandatory training, support will be provided by the Information Governance Officer and/or via the CHC Education team.

12.3 Document Accessibility

Further copies of current and archived policies can be obtained from the Policy Administrator including versions in large print, Braille and other languages.

13. Process for Monitoring Effective Implementation

The effective implementation of this policy will be monitored by the Data Protection Officer and the IG Forum. Any concerns can be escalated to an Executive Director but should be presented to the Data Protection Officer in the first instance.

14. Associated Documentation

This document references the following supporting documents which should be referred to in conjunction with the document being developed.

- Management, Storage and Destruction of Health Records Policy.
- Access to Health Records Policy.
- Your Information - Privacy Matters at Cornwall Hospice Care.

15. References

- Data Protection Act 2018.
- General Data Protection Regulation (GDPR) guidance @ ICO website https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

- ICO guidance "Subject access code of practice" @ https://ico.org.uk/fororganisations/guide-to-data-protection/principle-6-rights/subject-access-request/
- The NHS 'Guide to the Notification of Data Security and Protection Incidents' https://www.dsptoolkit.nhs.uk/Help/Attachment/148

Appendix 1 – Caldicott Principles

What are the Caldicott Principles?

The Caldicott Principles were developed following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out seven Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organisation should use the Principles as a test. The Principles were extended to adult social care records in 2000.

The Caldicott Principles revised 2013 are:

Principle 1 - Justify the purpose(s) for using confidential information
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share Or Not To Share? The Information Governance Review", informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

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

Appendix 2 - Consent

ICO Guidance on how to obtain, record and manage consent.

"In brief...

- Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand.
- Include the name of your organisation and any third parties, why you want the data, what you will do with it, and the right to withdraw consent at any time.
- You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or default settings.
- Wherever possible, give granular options to consent separately to different purposes and different types of processing.
- Keep records to evidence consent – who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.
- Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes."

Appendix 3 – "Right to be Forgotten"

Basically Data Subjects have the right to ask for all data about them to be removed/deleted (erased).

In general the Charity is content to comply with such requests provided that:

- It is lawful to do so.
- The Charity can still discharge its responsibilities to the Data Subject e.g. provide care.
- The data is not required in the defence of legal claims.

However, a skeleton record may be retained to prevent future data collection of the Data Subject's information.

Full text regarding the right to be forgotten - taken from Article 17 of the GDPR – this appendix should be replaced by a plain English version once available.

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

   (a) The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; 4.5.2016 L 119/43 Official Journal of the European Union EN.
   (b) The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing.
   (c) The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2).
   (d) The personal data have been unlawfully processed;
   (e) The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
   (f) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

   (a) For exercising the right of freedom of expression and information.
   (b) For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
   (c) For reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3).
   (d) For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.
   (e) For the establishment, exercise or defence of legal claims.

Appendix 4 – Information Incident Reporting Form

Location of incident:

Date of incident:

Which of the following best describes the incident *(please tick one):*

Lost digital equipment e.g. laptop computer	☐
Theft of digital equipment e.g. laptop computer	☐
Lost information (paper/digital e.g. USB stick)	☐
Theft of information (paper/digital e.g. USB stick)	☐
Information Breach - Post	☐
Information Breach - Email	☐
Information Breach - Fax	☐
Other Breach of Information Security	☐

Other (please specify):

Details of the incident (please focus on facts rather than opinions):

Immediate action taken (if any):

Further planned/required actions (if any):

Form completed by: _____ Date: _____

Please return to: **Richard Ward** (information Governance Officer)
rward@cornwallhospice.co.uk Tel: 01726 66868 Option 7

IG Use:

Action: Ref No:

Annex A - Your Information - Privacy Matters at Cornwall Hospice Care

This is a summary of the processing of personal information carried out by Cornwall Hospice Care (the Charity) and it is supported by more detailed information in 'Fair Processing' and 'Privacy' notices for many of the individual areas covered here. These Notices and policies are all available from the Charity's website (https://www.cornwallhospicecare.co.uk/home) or the Data Protection Officer who can be contacted at:

The Data Protection Officer
Mount Edgcumbe Hospice,
Porthpean Road,
St Austell,
PL26 6AB
Or:
InfoGov@cornwallhospice.co.uk

The Charity will comply with the requirements of the data protection legislation in force, including the Data Protection Act 2018, the UK General Data Protection Regulations and the Privacy in Electronic Communication Regulations (PECR).
All our information systems, paper and electronic, are designed to be secure and protect data from unauthorised access, theft and misuse.

Why do we need to process personal information?

We need to process personal data in order to deliver our services:

- In the provision and management of health, welfare and support services to patients.
- To provide, manage and develop Fundraising opportunities.
- To provide retail services.
- To manage the affairs of the Charity.

With the consent of patients and carers we collect the personal and sensitive information that we need in order to provide appropriate healthcare. For the purposes of care this information will be shared amongst the clinical team providing the care.

We process the personal data of staff and volunteers to:

- Recruit staff and volunteers

- Fulfil contractual requirements
- Meet legal requirements
- Provide effective management
- Develop a highly skilled and qualified workforce
- Deliver health, safety and welfare commitments.

The legal basis for such processing is a combination of legal requirements and legitimate interest and in some instances consent.

We also collect personal data from retail customers to:

- Fulfil contractual obligations
- Meet legal requirements

and supporters to:

- Respond appropriately to communications, donations and gifts
- Meet legal requirements
- Provide information about the activities of the Charity

The legal basis for processing supporter information is normally because of legal requirements or is a legitimate interest of the Charity.

Our Fundraising team may collect personal and sensitive information in the context of events held to support the Charity and keep potential event participants informed of future events.

The legal basis for collecting this information is usually the consent of the potential or actual participants of the events or to meet legal/contractual requirements. In the case of informing potential or actual participants of previous events of upcoming events the legal basis is one of legitimate interest.

The Lottery (and Raffle) activities of the Charity process personal information of participants to run these events and the legal requirement for retaining lottery data is extended to coincide with the retention period of finance records.

Recording personal information about you

Most information we hold will be collected from you but we may also obtain this from third parties such as your doctor (or other health professional) or other relevant organisation such as a previous employer for a reference.
We will always tell you why we need your information and how we'll use it. We will only ask you for information that is relevant and necessary to the delivery of our services. Information we hold about you will vary dependant on the contact you have with the Charity and the services we provide to you. For example if we are providing you with healthcare your information will be shared with those directly involved in providing that care. If we're supporting you with training, it's helpful that we know about your education and previous employment history. If you need adaptations in your workplace, we may need to know about associated health conditions.

Information Sharing

Sometimes we need to share your information with other organisations that we work with or who provide services on our behalf. We will only share relevant details and we will ensure your information remains secure.

We may need to share information in order:

- To provide you with the most appropriate healthcare
- To meet our legal obligations
- To fulfil a contract with you e.g. when we use a 3rd party to make a delivery
- In connection with legal proceedings (or where we are instructed to do so by Court order)
- To protect the vital interests of an individual (in a life-or-death situation)

When the information we need to share is defined as 'special' (e.g. information about health matters, ethnicity, religion, sexual orientation), we will generally ask you for consent before we share unless we are required or permitted to share this by law.

Your Rights

You can ask for a copy of the personal information we hold about you. This is known as a Subject Access Request (SAR). You can also request information to be corrected, erased or transferred to another organisation. You also have the right to be 'forgotten''. Please put all requests in writing (or email). Further details outlining all of your rights in relation to your personal data are available in our "Subject Access Request policy and procedure" which is available on our website.

Accurate and Up to Date

Please tell us if your information changes so we can keep it up to date. For example if you change your contact details including mobile number and email address. We won't keep your information longer than we need to. Our Data Retention Schedule outlines how long information is kept – and is published on our website.

Consent and Promotion of Our Services

We may use your contact details to send you information and communicate with you about matters associated with your connection to the Charity. We will not send you electronic 'direct marketing' unless you have agreed to this. We will never provide or sell your details to 3 parties for their marketing purposes. You have the right to object to direct marketing at any time, and our communications will always include clear instructions on how to 'unsubscribe'.

Appendix 5 - Equality Impact Assessment Form

Section One

<table>
<tr><td colspan="6">Name of the Policy to be assessed: Data Protection Impact Assessment Procedure</td></tr>
<tr><td colspan="3">Area responsible for completion:
Information Governance</td><td colspan="3">Is this a new policy? NO
A refresh of an existing policy? YES</td></tr>
<tr><td colspan="3">Name of individual completing EIA:</td><td colspan="3">Contact details:
R Ward
infoGov@cornwallhspice.co.uk</td></tr>
<tr><td colspan="2">1. Policy Aim. Who is the policy aimed at?</td><td colspan="4">This policy is aimed at all those with an interest in how the Charity collects, uses and eventually destroys personal data.</td></tr>
<tr><td colspan="2">2. Policy Objectives.</td><td colspan="4">To ensure compliance with Data Protection law.</td></tr>
<tr><td colspan="2">3. Policy intended outcomes.</td><td colspan="4">Compliance with UK Data Protection Legislation and to reduce the risk of a data breach occurring</td></tr>
<tr><td colspan="2">4. How will you measure the outcome?</td><td colspan="4">The number of reported data breaches will provide an indicator regarding the successful implementation of this policy.</td></tr>
<tr><td colspan="2">5. Who is intended to benefit from the policy?</td><td colspan="4">All data subjects</td></tr>
<tr><td colspan="2" rowspan="3">6. A) Who did you consult with?

B) Please list any groups who have been consulted about this policy.</td><td>Workforce</td><td>Patients</td><td>Local groups</td><td>External organisations</td><td>Other</td></tr>
<tr><td>n/a</td><td>n/a</td><td>n/a</td><td>n/a</td><td>n/a</td></tr>
<tr><td colspan="5">Please record specific names of groups:

None – this is a legal requirement</td></tr>
</table>

7. The Impact

Please complete the following table. If you are unsure/do not know if there is a negative impact you need to repeat the consultation step.

Are there concerns that the policy **could** have a positive/negative impact on:

Protected Characteristic	Yes	No	Unsure	Rationale for Assessment/Existing evidence
Age		✓		
Sex (male, female, non-binary, asexual etc)		✓		
Gender reassignment		✓		
Race/ethnic communities/groups		✓		
Disability (learning disability, physical disability, sensory impairment, mental health problems and some long-term health conditions)		✓		This policy applies to all people and is therefore consistent in its approach regardless of any of the Protected Characteristics
Religion/other beliefs		✓		
Marriage and civil partnership		✓		
Pregnancy and maternity		✓		
Sexual orientation (bisexual, gay, heterosexual, lesbian)		✓		

If all characteristics are ticked 'no' and this is not a major working or service change, you can end the assessment here as long as you have a robust rationale in place.

Name of person confirming result of initial impact assessment and date:	Name R Ward	Date 24/3/2023