CHILDREN'S HOSPICE SOUTH WEST

DATA PROTECTION POLICY
HR/DP/18

Section 1 Policy administration

Approved By / Include Date:	Approved by Executive: Sept 2013 (Note: This policy replaces **Employment** Data Protection Policy HR/DP/18) Approved by the Board: March 2017 Approved by the Board: November 2018 Approved by the Board: October 2022
Policy Sponsor:	Chief Executive
Originator:	Director of HR
Responsibility for Dissemination:	Senior and Line managers
Compliance:	All employees, managers, volunteers or anyone else processing information on behalf of CHSW.
Policy Monitoring and Review:	The Director of HR will meet with SMT at 4 yearly intervals and review the effectiveness and quality of this policy or sooner if appropriate.
Policy Version:	October 2022
Expected Review Date:	October 2026

Section 2 – Policy scope

Scope:	This policy applies to all CHSW employees and volunteers including Trustees, contractors, consultants and temporary appointments (collectively known a staff) and any other representative who collects and processes data on behalf of CHSW, and all data held electronically or in manual files.
Policy statement:	This policy is to ensure that CHSW : • Complies with the law. The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 • follows good practice • protects clients, staff and other individuals • protects the organisation This policy also sets out CHSW's approach to dealing with Data Protection Subject Access Requests and breaches.
Related hospice policies/procedures:	Acceptable Use of IT policy Policy & Procedure for Children & Families: Access to Health records / Care/015 Policy & procedure for Health records: Creation, Management, Storage and Destruction / Care/016 Records Retention Policy & Procedure Social Media Policy Employee Handbook/Induction Handout Volunteer Handbook/Induction Handout Training Programme(s) Recruitment and Selection Policy Employment References Policy Confidentiality Agreements for Third Party Suppliers; Information Governance Policy
Compliance with statutory requirements	UK GDPR DPA 2018 ICO Data Protection Employment Practices Code Regulatory of Investigatory Powers Act 2000 Crime and Disorder Act 1998 Human Rights Act 1998 Equality Act 2010 Police and Criminal Records Act 1984 Access to Health Records Act 1990 Access to Medical Reports Act 1988 Payment Card Industry Data Security Standard (PCI DSS)
Privacy Impact Assessments	Low Risk – no full DIPA required

Section 3 – Contents

Section 4 – Policy

4.1 Introduction

The UK Data Protection Regulation (UK GDPR) and the Data Protection Act (2018) (DPA) together provide the legal framework for data protection.

The UK GDPR sets out the key data protection principles, rights and obligation for the processing of personal data/ The DPA supplements the UK GDPR and contains exemptions to some of the rights and obligations provided by the UK GDPR

The UK GDPR requires a more proactive, systematic and accountable attitude towards data protection compliance and is concerned with the rights of individuals when processing their information. This is achieved by being open and honest with employees about the use of information about them and by following good data handling procedures.

The regulation is mandatory and all organisations that hold or process personal data must comply. Both employers and employees have new responsibilities to consider, to help ensure compliance. Organisations must have a valid reason for having personal data and the data should not be held for any longer than necessary.

This policy also covers the **Payment Card Industry Data Security Standard** (PCI DSS) which refers to payment security standards that ensures CHSW safely and securely accepts, stores, processes, and transmits cardholder data during a credit card transaction. Further specific details can be found in Appendix 4

4.2 Policy statement

Under the UK GDPR CHSW, is a data controller, registered with the Information Commissioners Office (ICO). CHSW collects and processes personal data and is committed to being transparent about how it collects and uses the data and to meeting its data protection obligations.

CHSW regards the lawful and correct treatment of personal information as extremely important to successful working and to maintaining the confidence of those with whom we deal.

a) CHSW is committed to:
    - having a valid reason for having personal data and not holding onto it any longer than is necessary;
    - respecting individuals' rights when processing their information and preventing harm to individuals;
    - complying with both the law, UK and European Regulations, and good practice;
    - applying Data Protection Impact Statements (DPIA) when processing is "likely to result in a high risk to the rights and freedoms of natural persons" in particular when looking at new processing activities, a new system or where an activity may be outsourced to a third party;
    - being open and honest with individuals whose data is held;
    - providing training and support for individuals who handle personal data for CHSW, so that they can act confidently and consistently.

b) CHSW recognises that its first priority under the DPA/ UK GDPR is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands;
- holding good quality information.

Secondly the DPA/ UK GDPR aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, CHSW will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

c) This policy applies to all personal data and special category personal data collected and processed by CHSW in the conduct of its business and applies to both automated personal data and to manual filing systems.

d) This policy applies to all CHSW employees and volunteers including Trustees, contractors, consultants and temporary appointments and any other representative who collects and processes data on behalf of CHSW, and all data held electronically or in manual files.

e) The day-to-day management of data protection rests with the managers holding or processing personal data.

f) Subject Access Requests will be initially dealt with by Human Resources who will work with the specific department(s) where the requested data is held.

g) CHSW staff should be aware that a breach of this policy could result in disciplinary action being taken.

h) All contractors, consultants, partners or agents of CHSW should be made aware that any breach of any provision of the DPA/UK GDPR will be deemed as being a breach of any contract between CHSW and that individual, company, partner or firm and may be reported to the Information Commissioners Office (ICO).

i) CHSW will carry out spot checks across all sites from time to time as part of its monitoring and audit process.

j) A relevant Privacy Notice will be made available to all CHSW staff and volunteers. The most recent version will always be available on CHSW's intranet/internet.

k) A copy of the Data Protection Policy is also available on the intranet under HR Policies, or from the local HR Office.

l) In addition, staff and volunteers have access to CHSW's Privacy Policy on the public website www.chsw.org.uk

4.3 Key Definitions

a) **Personal Data**

Personal data means any information relating to an identified or identifiable living individual person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity.

Personal information can be factual i.e. address and date of birth, or it can be an opinion i.e. information relating to the services which individuals receive from CHSW or comments in a staff's personal development review.

Staff should note that any personal data in their possession is also subject to the regulation e.g. if a manager has a written copy of contact details of their team or an employee keeps family names and numbers on post it notes on their desk.

Individuals who hold data about another individual on a personal level, e.g. family members telephone number stored in a phone, will not need to consider UK GDPR.

b) **Special categories of personal data**

Data relating to an identifiable, living individual relating to racial or ethnic origin; political opinions; religious or philosophical belief; trade union membership; genetics; biometrics; physical or mental health condition; sexual life; sexual orientation criminal offences.

Such data is given higher levels of protection.

c) **Processing** any activity that involves the data i.e. collecting, holding, recording, sending, analysing, using, retrieving, storing, updating, disclosing or destroying the data.

d) **Data Controller –** CHSW is the Data Controller under the UK GDPR which means that it determines how and why personal data is processed.

e) **Data Subject** – an individual who is subject of personal data e.g. employees, former employees or job applicants.

f) **Data Processor** - any person or organisation that process information on behalf of the Data Controller (CHSW).

g) **ICO** – The Information Commissioners Office, the authority within the UK which is tasked with the protection of personal data and privacy. The ICO is the UK's supervisory authority for the purposes of UK GDPR.

h) **DPO** – Data Protection Officer plays a crucial role in helping CHSW fulfil its data protection obligations and is involved closely and in a timely manner, in all Data Protection matters i.e. assists to monitor internal compliance, informs and advises on CHSW's data protection obligations, provides advice regarding DPIAs and acts as a point of contact for data subjects and the ICO.

4.4 Principles

a) As CHSW keeps information about individuals we must comply with the DPA/UK GDPR. These outline principles which underpin the handling of personal data. CHSW must ensure that personal data is:

1. **Processed fairly, lawfully and in a transparent manner in relation to individuals** Individuals should be advised why the information about them is required, how it will be used and anyone the information may be disclosed to.

2. **Collected for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes**
Personal information should only be used for the purpose it was intended for, it should not be used for other purposes unless a legal exemption applies or if further consent/ permission has been provided;

3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**
CHSW must be able to objectively justify the relevance of personal information held and should not be excessive in relation to the purposes for which it is held;

4. **Accurate and where necessary kept up to date**
CHSW is obliged to ensure the data it holds is accurate and up to date; every reasonable step is 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;

5. **Not kept longer than is necessary**
Personal information should be reviewed on a regular basis and out-of-date or irrelevant information should be deleted or destroyed. Please see CHSW's Records Retention Policy and Procedure for further guidance and retention periods;

6. **Processed in a manner that ensures security of personal data including protection against unauthorised, or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures**
Manual information should be locked, in some cases locked within a cabinet within an attended or locked office. Electronic information should be protected by passwords and USB sticks encrypted. Personal information should not be discussed or disclosed to other individuals who do not have a legal right to know;

7. **Processed in accordance with the rights of the data subject**
As a data subject, individuals have a number of rights. They can:

- Obtain a copy of information held about them that identifies them as an individual. This right is called 'Subject Access' and CHSW is expected to provide a copy of their information upon request (see Section 5.7). There may be some exemptions to this, and it is important to advise Human Resources of any Subject Access requests to be handled;

- Individuals also have the right to have inaccurate or incomplete data held about them changed, deleted or destroyed and could claim compensation for any damage or distress caused;

- Require CHSW to delete or stop processing their data, for example where data is no longer necessary for the purposes of processing;

- Object to the processing of their data where the organisation is relying on its legitimate interests as the legal ground for processing;

- Lodge a complaint with a supervisory authority;

- Not be subject to automated decision making, including profiling, which has legal or other significant effects on them; there are some exceptions e.g. where explicit consent has been given or where it is necessary for entering into or performing a contract. However, even where an exception is relied upon, additional safeguards are required e.g. the right to require human intervention in the process.

8. **Transferred only to countries with adequate security.**
Personal information will not be transferred to a territory outside the European Economic Area (EEA) unless that country ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

4.5 Responsibilities

a) Trustees:
Recognise their overall responsibility for ensuring that CHSW complies with its legal obligations.

b) Department Heads and Line Managers:

- Managers have a responsibility for the type of personal data they collect and how they use it;
- Managers of departments where personal data is handled, are responsible for drawing up their own departmental operational procedures (including departmental induction and training) to ensure that good data protection practice is established and followed;
- must ensure that Human Resources is informed of any changes in their uses of personal data that might affect the organisation's registration;
- demonstrate their commitment and support to this policy;
- reflect the policy and procedure within their own management practice and regularly review and audit the way they hold, manage and use personal information;
- know when and where to seek additional advice and support.

c) Individual staff and volunteers are expected to:

- Ensure that their activities comply with the data protection principles.
- Read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work;
- Communicate effectively with their manager on an ongoing basis and raise any issues of concerns or data protection incidents as and when they occur;
- Co-operate fully with any organisations that provide support to CHSW and its employees in relation to this policy and procedure;

- Not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

- Ensure their own personal data held by CHSW is accurate and up to date, for example, title, name, address, contact details, next of kin, emergency contact(s) etc. via their self- service access of the HR System (Cascade), and/or informing their line manager of any changes.

d) CHSW has a responsibly to make any Contractor, Agent or anyone else processing information on behalf of CHSW aware that:

- They must comply with this policy, with specific regard to section 5.10;

- All third parties who are users of personal information supplied by CHSW will be required to confirm that they will abide by the requirements of the DPA/UK GDPR with regard to information supplied by CHSW;

- They must allow data protection audits by CHSW of data held on its behalf (if requested).

Section 5 – Procedure

5.1 Checklist before processing data

Before processing personal data individuals should consider:

- Is it necessary to record this information?

- Has the data subject been told that this information will be processed and why? Eg Privacy Notice)

- Is the data accurate?

- Is the data secured? (see section on 5.2 Security)

- If you are processing personal data on behalf of another Data Controller for example, the police, fire or probation service, you should process their data only in accordance with their instructions.

5.2 Personal data security

a) All personal data whether manual or electronic must be kept secure to prevent accidental loss, damage or destruction. The extent of the security measures required will depend on the sensitivity of the data.

b) Paper records should be locked away in desks, filing cabinets or cupboards when they are not in use. The keys should be kept in a safe place.

c) If the data is electronic, access should be password protected. CHSW IT users must not share their user ID or passwords. PC screens should be situated so that they cannot be viewed by unauthorised personnel and users must log out of PC's when not in use, or lock PC using the Ctrl, Alt and Delete keys.

d) When records containing personal information have reached the end of their life, they will be disposed of by shredding, incineration or using confidential waste bins.

e) Personal data should not be sent by email where its security cannot be guaranteed

f) All USB sticks must be encrypted before they are used.

g) If CHSW users are required within the course of their duties to transfer personal data between sites or take it home (including laptops etc.), upmost care must be taken to keep the information secure and out of sight, and stored securely when left unattended.

h) If personal data is to be sent externally ensure the information is made secure and clearly marked 'Confidential' and where possible use registered post or courier service to transport the data.

i) We must at all times treat people's personal information as we would wish our own to be treated.

Further information regarding the retention, storage and disposal of personal data can be found in the CHSW policies on Data Retention and the Acceptable Use of IT Policy.

5.3 Accuracy of data

a) It is the responsibility of those who receive and process information to ensure, as far as possible, that it is accurate, valid and up to date;

b) Individuals who input or update personal information must ensure it complies with the principles of data protection described at 4.3. If an individual is aware that information recorded is inaccurate they must take steps to rectify it;

c) Individuals must be aware that any information which they record about someone (whether in a handwritten note, email or more formal document) may be disclosed to that person upon request (Please see 5.7 Subject Access).

5.4 Revision and destruction of data

a) Personal information should not be kept for longer than is necessary. Information and associated retention periods should be reviewed at frequent intervals to ensure they are up to date and still relevant. If personal data is no longer needed and there is no legal or other reason to hold the information, it should be destroyed. Please also refer to CHSW's Records Retention Policy.

5.5 Access, use and disclosure of personal information

a) Access to and use of personal information on behalf of CHSW must only be done in relation to individual official duties. Use of this information for any other purpose is prohibited and improper use or disclosure may result in disciplinary action.

b) Personal information held by CHSW must not be disclosed to anyone internally, or externally, unless the disclosing individual is fully satisfied that the enquirer is fully authorised and legally entitled to the information. If possible, requests for information should be in writing stating their reasons and legal entitlement to the information. Checks on the identity of the enquirer should also be made. Individuals should be aware that other individuals or organisations may try to trick CHSW into giving away information. If you are not sure you must seek guidance from your line manager or Human Resources.

c) In response to a lawful request, only the minimum of personal data should be disclosed. The information should be adequate for the purpose of the disclosure, relevant and not excessive.

d) Individuals must take particular care when disclosing personal data to third parties, to ensure that there is no breach of the DPA/UK GDPR or of confidence. Disclosure may be unlawful even if the third party is a family member of the data subject, or a local authority, government department or the police. A key point to consider is whether the disclosure is relevant to and necessary for the conduct of CHSW's business. For example, it would generally be appropriate to disclose a staff member's work contact details in response to an enquiry relating to a function for which they are responsible, but it would not be reasonable or appropriate to disclose a staff member's personal address or bank account details.

5.6 Non-disclosure exemptions

There may be occasions when CHSW obtains personal information for one purpose then needs to use it or disclose it for another purpose. The DPA/UK GDPR also allows personal data to be disclosed to third parties without the consent of the data subject, in the following circumstances:

- The disclosure is necessary for safeguarding national security;
- The disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders;
- The disclosure is necessary for the assessment or collection of any tax or duty;
- The disclosure is necessary for the discharge of regulatory functions (including the health, safety and welfare of people at work);
- The data to be disclosed are to be used for research purposes, subject to the rules governing the use of personal data in research;
- The data are information which CHSW is obliged by legislation to provide to the public;
- The disclosure of the data is required by legislation, rule of law or the order of a court.

In these cases, advice should always be sought from Human Resources before making a disclosure.

5.7 Right of access to personal information: subject access

a) Individuals (data subjects) have a right to receive a copy of personal information held about them (subject access right) by CHSW subject to certain exemptions.

b) Individuals should complete CHSW's subject access request form (Appendix 1) when making any request and forward to Human Resources, although this is not compulsory.

c) All CHSW staff must know how to recognise a subject access request and realise that it must be dealt with urgently. The request may not mention the DPA/UK GDPR, it may just say 'I want to see all the information you hold about me'. Any member of staff who receives a subject access request must immediately contact Human Resources and provide details of the request.

d) CHSW is obliged to provide a copy of the requested information, subject to certain exemptions, within one month of receiving the request.

e) CHSW may request a fee should an individual make repeated or excessive requests.

5.8 Fair processing of information

a) Whenever personal data is collected, we must provide the Data Subject with information about our intentions with their data, this is known as a Privacy Notice.

b) We must inform the Data Subject of the identity of the Data Controller (CHSW), the purpose(s) for which the information is to be used and with whom the information may be shared.

c) The Data Subject should be given the opportunity to opt out of having their data used for other purposes. This can be achieved by use of an opt out 'tick box'.

d) A list of individuals who have opted out should be kept and checked whenever necessary. If an individual receives information after specifying that they do not want it, the DPA/UK GDPR have been breached.

e) Standard privacy statements will be provided for use on forms where data is collected.

f) Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

g) When using mailings (electronic or postal) from CHSW e.g. for marketing purposes, CHSW will make our identity clear, provide a valid address for opt-out requests and not send unsolicited marketing material unless the recipient has previously consented to receiving such material.

5.9 Awareness, training and acceptance of responsibilities

a) CHSW will ensure responsibility for maintaining awareness of confidentiality and data protection for all staff and volunteers including:
- Personal responsibilities;
- Confidentiality of personal information;
- Relevant CHSW policies and procedures;
- Individual rights (access to information and compliance with the principles);
- General good practice guidelines covering security and confidentiality;
- Awareness to all staff about who the DPA/UK GDPR Leads are and how they can be contacted.

b) Information for staff is contained in the staff handbook and both staff and volunteers in the guidance leaflet *Guidance for all staff, volunteers and contractors on handling personal information (Appendix 2)*

c) All staff and volunteers who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.
d) Data protection and security will be included in mandatory training for all staff and volunteers of CHSW.
e) Staff agree to comply with this policy under the terms of their employment contract.

5.10 Third party processing

a) Where a third-party processes personal data on behalf of CHSW, e.g. web site hosting, service provider, CHSW must:

- obtain a 'Confidentiality Agreement' (or other) for Third Party Suppliers which will provide a contract under which the data processor is to act only on instruction from CHSW;
- choose a data processor providing sufficient guarantees in respect of the security measure they take.

b) Take reasonable steps to ensure compliance with those measures.

c) Personal data must not be transferred to a country outside of the European Economic Area (EEA) unless that country ensures an adequate level of protection. If you are required to deal with such arrangements seek advice from the Human Resources.

d) Where we are processing data on behalf of another Data Controller for example the police, fire or probation service, we should process their data only in accordance with their instructions.

5.11 Data Breach

a) A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Simple mistakes can lead to breaches, for example, losing a memory stick, leaving a laptop on a train or sending an email to the wrong person. A breach is more than just about losing personal data for example, confidential information left on printers, personal information left in cars on view.

b) Under the UK GDPR CHSW has a duty to report certain types of personal data breach to the relevant supervisory authority and the affected individuals. This must be done within 72 hours of becoming aware of the breach, where feasible. Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2% of turnover. CHSW must therefore, keep a record of any personal data breaches regardless of whether notification is required. For non-care related breaches, staff must complete a Data Breach Form which can be accessed via the CHSW intranet **http://intranet/GDPR/default.aspx ,** along with the flow chart, on each occasion a data breach occurs; this then informs key people who make a decision as to whether the breach needs to be reported. For care related breaches recording is made via the Accident Incident and Near Misses (AINMS) system and highlighted immediately as such to management.

c) An individual who suffers damage or distress as the result of any breach of the requirements of the DPA/UK GDPR by a Data Controller, is entitled to seek compensation through the Courts.

d) An individual who believes they have been affected by the processing of personal data, may ask the Information Commissioner to assess whether or not the processing of the data has been carried out in compliance with the DPA/UK GDPR.

5.12 Monitoring and audit

a) This Policy and Procedure will be monitored by the Director of Human Resources and the Information Governance Committee and will meet with SMT at 4 yearly intervals and review the effectiveness and quality of this policy or sooner if appropriate.

b) Managers and those responsible for their departmental procedures and guidelines will review the effectiveness of their processes annually or where required e.g. introduction of changes to what data is accessed or processed.

Section 6 – Further Guidance

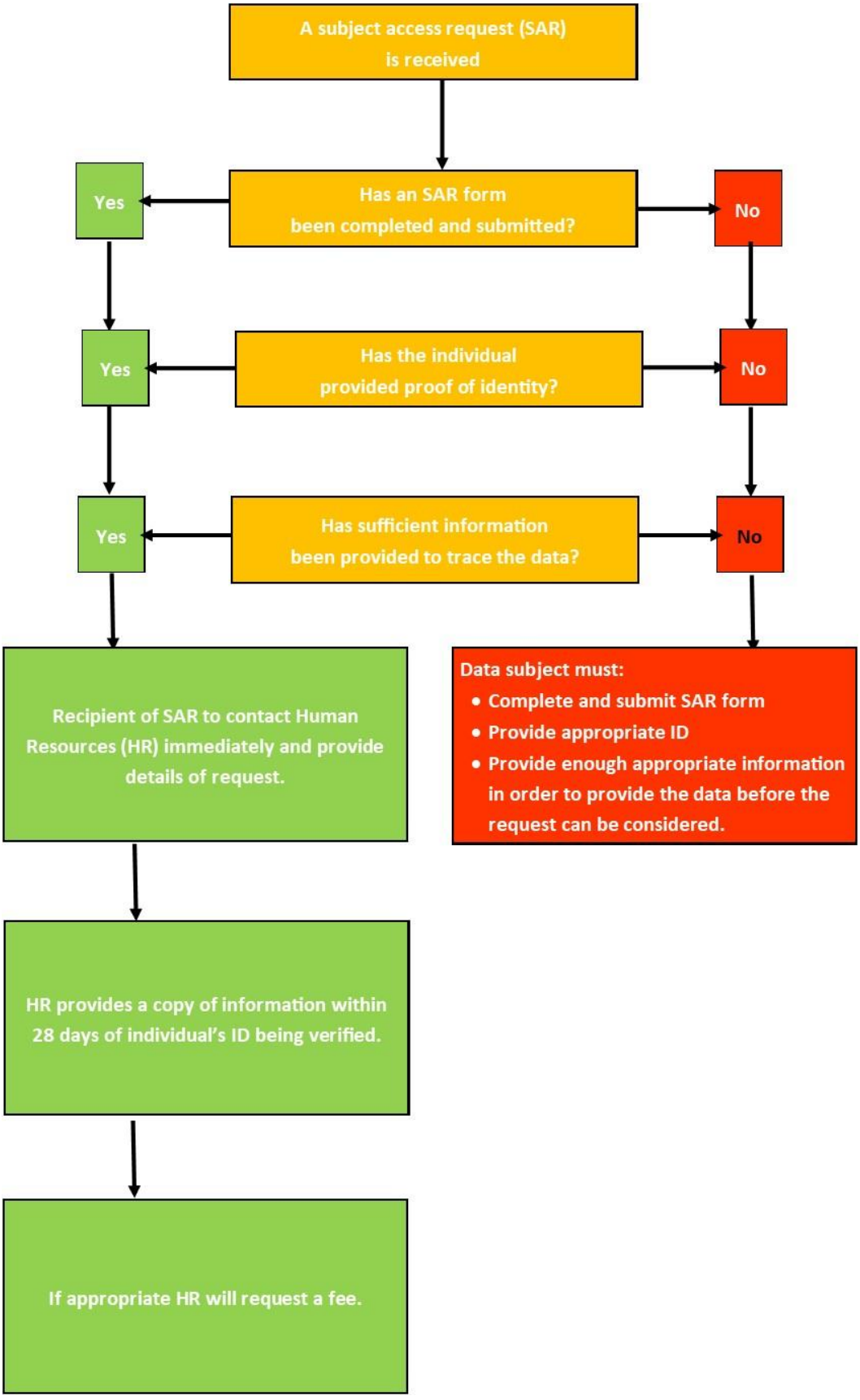
Further information on the DPA/UK GDPR can be found at:

Information Commissioner's Office (the UK's independent authority set up to promote access to official information and to protect personal information) website: www.ico.gov.uk

Policy History

Policy Date	Summary of Change	Contact	Version/Date	Review Date
Sept 2013	New Policy: This policy + Data Protection Procedure: Subject Access request replaces **Employment** Data Protection Policy HR/DP/18)	HR	Sept 2013	Sept 2106
Sept 2013	Review only. Minor tweaks to job titles and associated policies.	Daphne Sands HR	March 2017	Mar 2021
March 2017	Review following the GDPR which came into force on 25th May 2018	Daphne Sands HR	November 2018	July 2022
Oct 2022	To include reference to Payment card devices and cardholder date to support PCI DSS requirements To update with reference to new UK GDPR and DPA (2018)	Jess Patel Marketing	Oct 2022	Oct 2026

Appendix 1 – CHSW Subject Access Request (SAR) Flow Chart



Appendix 1 - Subject Access Request Guidance and Form

Guidance:

a) **About Yourself** - asks you to give information about yourself which will help Children's Hospice South West to confirm your identity. We have a duty to ensure that the information we hold is secure and so we must be satisfied that you are who you say you are.

b) **Proof of Identity** - asks you to provide evidence of your identity by producing TWO official documents (which, between them, show your name, date of birth and current address). Photocopies are acceptable.

c) **Information Requested** - you must indicate what type of information you are looking for.

d) **Declaration** - must be signed by you or someone authorised on your behalf. Any third party making a request on your behalf CHSW will need to be satisfied that they have the authority to do this. This would normally be via written authority or power of attorney.

e) When you have completed and checked this form, send it together with copies of the required identification to the appropriate HR Team member.

Subject Access Request Form

About Yourself

The information requested below is to help Children's Hospice South West satisfy itself of your identity and to find any personal data held about you.

PLEASE USE BLOCK LETTERS

Title (tick box if appropriate): Mr ☐ Mrs ☐ Miss ☐ Ms ☐	
Other Title (e.g. Dr, Rev etc.):	
Surname / Family Name:	
First Name:	
Maiden / Former Names (if changed during employment):	
Date of Birth:	
Your Current Home Address (to which we will reply)	A telephone number will be helpful
Address:	Telephone Number:
	Alternative Number:
Postcode:	

Proof of Identity (required from individuals not currently employed by CHSW)

To help establish your identity if you are not currently working for CHSW, your application must be accompanied by TWO official documents which, between them, show your name, date of birth and current address. Photocopies are acceptable. For example: A birth certificate/adoption certificate, driver's licence, medical card, passport or any other official document which shows your name and address. Failure to provide this proof of identity will delay your application.

PLEASE COMPLETE THIS SECTION AS FULLY AS POSSIBLE
Information Requested

To ensure that we provide you with the right information, please state below exactly what information you would like us to look for. Please don't just ask for "everything you hold on me".

If you would like a copy of a particular file/document, then please state this below. Additionally, if you do not want particular information then please let us know. If you narrow your request to the specific information that you want, this will help us provide it to you much quicker.

Please provide me with the following information:

Upon receipt of your identification, we have a statutory time limit of one month within which we must provide you with the information that you have requested.

Declaration

The information that I have supplied in this application is correct. *I am the person to whom this request relates / *I am authorised to act on behalf of the person to whom this request relates. *please indicate correct answer

Signed by: ……

Dated: ……

Before returning this form, please check that you have completed ALL the sections, have enclosed copies of TWO identification documents of yourself, have signed and dated the application form.
If you have any queries regarding this form, contact your local Human Resources Department:
Little Bridge House – 01271 313310
Little Harbour –-01726 871800
Charlton Farm – 01275 866600

Office Use Only

Date application was received:	
Who received the request?	
Application checked and legible?	Yes / No
Identification documents checked?	Yes / No / not applicable
What identification was provided?	
Identification documents returned?	Yes / No / Not applicable

Appendix 2 - **Guidance for all staff, volunteers and contractors on handling personal information**

This leaflet sets out your responsibilities when handling personal information.
All staff will at some point use personal information. Failure to handle information appropriately may affect the care of our children, CHSW's reputation and lead to legal action or a significant fine. Deliberate inappropriate use is likely to lead to disciplinary action. If in doubt, always seek advice.

This leaflet is a brief summary of your responsibilities with regard to personal information. If unsure how to handle information, please seek advice. Your line manager can direct you, or speak to Human Resources.

Definitions and responsibilities
Personal information
Information about an individual, which includes either some or all details of their identity is personal and is subject to the DPA/UK GDPR.

Confidential or sensitive information
Personal information, in any form is confidential. This means that information should only be shared or accessed by someone with a legitimate reason and related to the activity the information is being requested for i.e. the care of a child or donor/supporter request. Information about members of staff or others in relation to sensitive issues, such as appraisals or payroll details is also confidential.

Protecting information (including personal and sensitive data)
Keep information secure and available

- Do not share your passwords
- Only access information about individuals where you have a justified work-related reason to do so
- Only store personal information on electronic media such as a memory stick and always ensure that it is encrypted and only when necessary
- Ensure that personal information contained in emails is sent by a secure method
- Do not leave personal information lying around where it can be seen, read or removed by others
- Personal information or sensitive details should be marked as 'private and confidential'
- Lock record stores and filing cabinets and log-out of computer systems when they are not in use
- Ensure that if you transport information in any form (paper or electronic), it is kept secure at all times
- Ensure you are aware of any security requirements when handling information outside of your normal workplace, such as at home or other location. You may not transfer information onto any personal computer equipment that you own
- Dispose of personal or confidential information via confidential waste facilities

Record information accurately and consistently

- Record information onto paper or enter it into the computer as soon as possible
- If hand writing a record, make sure that it is legible
- Check individuals' personal details with them to ensure that they are up to date
- Any alteration or addition on a paper record must be dated, timed and signed
- Record relevant and useful information. Do not use unnecessary abbreviations or jargon and do not include irrelevant speculation or personal opinions

Only disclose sensitive information after thought and care

- Confirm the identity of anyone asking for information over the phone and if appropriate call them back to ensure they are who they say they are before releasing any data
- Ask them what they need and why they need it, so you can determine if it is appropriate to provide it to them
- Respect the sensitivity and privacy of individuals; ensure you are not overheard by others during private phone calls or conversations
- Establish the service user's wishes with regard to giving information to family and friends

Using personal information

- Justify why any personal information needs to be used. Seek advice if you need to use any information that could be used to identify a person.
- Only use personal information if necessary and always use the minimum amount of personal information required for the purpose

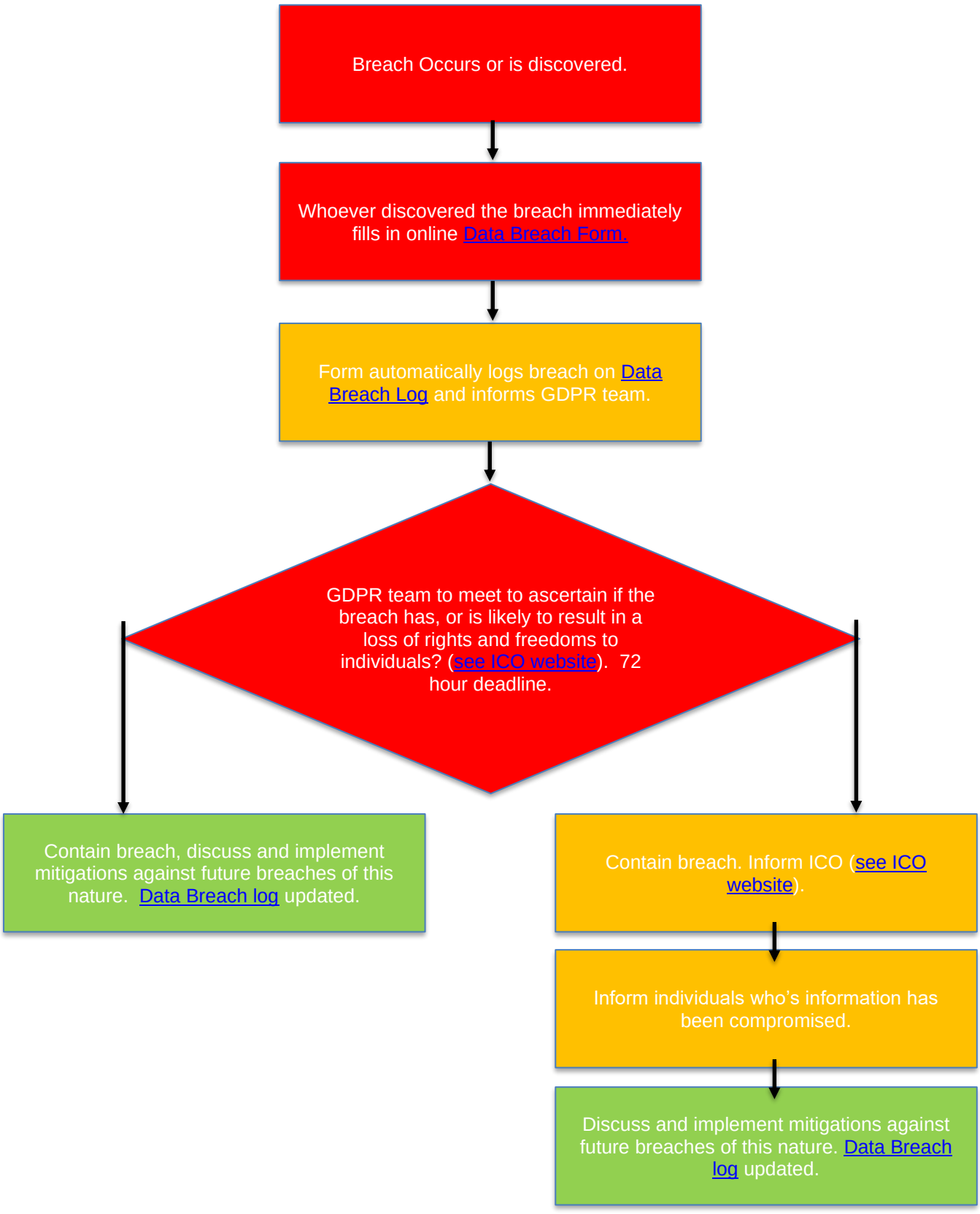
When deciding whether to share information

- Ensure that a request is lawful and reasonable
- When information needs to be shared about an individual who is not able to give consent and/or has difficulty understanding, ensure that it is in their best interests to do so
- Share the minimum information required to provide the necessary care or to satisfy a lawful, reasonable request
- Ensure information sharing is timely

Further information and guidance can be found in the following CHSW documents:

- Use of internet, email and telephone policy & procedure and Social Media Policy
- Care - Policy & procedure for Children & Families: Access to Health records
- Care - Policy & procedure for Health records: Creation, Management, Storage and Destruction Records Retention Policy & Procedure (DP/02)
- Employee Handbook

Appendix 3 – CHSW Data Breach Flow Chart (non-care related)



Appendix 4

Sensitive Cardholder Security and Usage

Children's Hospice South West handles sensitive cardholder information daily. Sensitive information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the Organisation.

Children's Hospice South West is committed to respecting the privacy of all of its supporters/customers and to protecting any data about customers from outside parties. CHSW are committed to maintaining a secure environment in which to process cardholder information so that we can meet this commitment.

Employees handing sensitive cardholder data should ensure:

- Company and cardholder information is handled in a matter that fits with their sensitivity
- Personal cardholder information is not disclosed to any third party
- Sensitive cardholder information is protected

Protect Stored Data

All sensitive cardholder data stored and handled by the Company and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the Company for business reasons must be discarded in a secure and irrecoverable manner.
If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, Messenger etc.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

Access to sensitive cardholder data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.

- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- CHSW will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- CHSW will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- CHSW will have a process in place to monitor the PCI DSS compliance status of the Service provider.

Physical Security

- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.

Protect data in transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.