People Policy on Confidentiality and Data Protection V2

This policy:

- Applies to all Colleagues, volunteers, agency workers and those on placement (known as "people" for the purposes of this policy)
- Applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject
- Replaces the People Policy on Confidentiality & Data Protection (last reviewed November 2017)
- In compliance with the No Life Half Lived Strategy: *"To be effective and accountable in all that we do."*
- Does not form any part of the Colleague's contract of employment and we may amend it at any time.

In line with our commitment to equal opportunities, this policy can be made available in a variety of formats, including large print, translated into another language or other media. Reasonable adjustments will also be made where required to assist people who have a disability.

We will endeavour to develop fair and consistent policies, procedures and practices to support our aims, values and objectives.

1. Our Human Rights Approach

1.1 We recognise everyone's individual rights and freedoms. They are based on important principles such as dignity, fairness, respect and equality.

1.2 In developing a human-rights based approach, this means that colleagues, volunteers, agency workers, service users and peer support groups have been fully supported to participate in the development of this policy.

2. Our Values

2.1 Our values are at the heart of what we do. We also recognise that people are the most important asset in achieving No Life Half Lived in Scotland.

3. Statement of Intent

3.1 Chest Heart & Stroke Scotland (CHSS) is an independent Scottish charity, whose aim is to improve the quality of life for people in Scotland after stroke, or diagnosis of a chest or heart condition. We offer vital advice, support and information to those affected, arrange group and 1-to-1 support in the community and influence public policy to ensure that people get the services they badly need. Our renewed ambition is to become Scotland's leading organisation for person-centered, user-led community support for people with our health conditions.

3.2 To operate and provide services, CHSS needs to collect and process relevant information (data) about its employees, volunteers, supporters, service users and others. By law, CHSS is obliged to comply with the UK General Data Protection Regulations (UK GDPR) which is the the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*).

3.3 We recognise that data management, protection and confidentiality are important to the work we do. We also recognise the importance of protecting the rights of individuals in respect of any personal information we keep about them.

3.4 This policy aims to uphold the principles of data protection (see '4 General Principles of the UK GDPR') and how we process data in accordance with the rights of individuals. This Policy sets out what we expect from you in order for CHSS to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

3.5 The Data Controller is Chest Heart & Stroke Scotland. Overall responsibility for ensuring that the charity complies with its data protection obligations rests with the Data Controller.

3.6 The Director of Finance & ICT is the Data Protection Officer (DPO) and is responsible for overseeing this Data Protection Policy, and will handle Data Protection matters and encourage good information handling practice within CHSS. Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

4. General Principles

4.1 We are required to follow the following principles in accordance with Article 5 of the UK GDPR:

- Lawfulness, fairness and transparency – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- Purpose limitation – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. CHSS practices in this matter will be compliant with UK GDPR Privacy by Design requirements.
- Accuracy – Personal data shall be accurate and, where necessary, kept up to date. Data that are inaccurate for the purposes they are intended must be updated or deleted without delay.
- Storage limitation – Personal data shall be 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.
- Integrity and confidentiality – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- Transfer Limitation - Not transferred to another country without appropriate safeguards being in place.
- Data Subject's Rights and Requests - Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.
- Accountability – The Data Controller shall be responsible for, and be able to demonstrate compliance with the UK GDPR principles

4.2 CHSS as the Data Controller shall be responsible for, and be able to demonstrate, compliance with these principles.

4.3 CHSS will ensure that we comply with legislation which governs all policies where we gather, handle, retain and destroy data.

4.4 The 'people' identified within this policy will maintain confidentiality both whilst performing their duties and after their role has ended.

4.5 A list of definitions referred to in the UK GDPR legislation is attached as Appendix 1.

4.6 This policy will in no way affect the rights of disclosure of information under our Whistleblowing Policy.

5. Responsibilities for Compliance with this Policy

Chest Heart & Stroke Scotland

5.1 CHSS recognises its ultimate responsibility for protecting the rights of individuals and their privacy with respect to the processing and security of their personal data and providing appropriate staff training. We will also regularly test our systems and processes to assess compliance.

5.2 Under the terms of the UK GDPR, CHSS is the Data Controller and responsibility for compliance lies with CHSS

5.3 Managers and Heads Of within CHSS have a responsibility to ensure good practices are adhered to for data gathering and management within their areas, and to ensure their staff have appropriate training for the tasks they carry out when handling data.

5.4 CHSS will abide by the UK GDPR requirements to be Privacy by Design compliant. This is an approach to projects that promotes privacy and data protection compliance from the start.

5.5 CHSS will be responsible for running Data Protection Impact Assessments (DPIAs) (also known as privacy impact assessments or PIAs) as required.

CHSS Departmental Responsibilities

5.6 It will be the responsibility of each Director, Head of and Manager to ensure that this policy and associated procedures are applied within their own department.

5.7 Each Director has specific responsibilities for personal and sensitive information held within their department.

5.8 Each Department will identify who, as part of their role, has responsibility to ensure compliance with this policy and will:

a) Audit data.
b) Check data for quality, consistency and duplication of personal data within their department.
c) Promote security of personal data.
d) Promote the UK GDPR principles in the Department.
e) Review the registration criteria within their department and advising the Director of Finance & ICT of any proposed amendments on an annual basis or more often if required.
f) Ensuring Subject Access Requests within their own department are responded to.
g) Reviewing the retention periods of data.

Staff and Volunteer Responsibilities

5.9 Before handling personal or sensitive data, you must have been formally trained to do so.

5.10 When processing data, you must comply with the guidance as set out in this document.

5.11 Your role may involve receiving, recording, collecting, maintaining and processing personal and sensitive data and you are responsible for following this policy and legislation, including ensuring the security of this data. If you are unsure about any of these aspects, you should seek guidance from your Line Manager.

5.12 Where you gather information, you must keep some form of record of how and when the data was captured and what legal basis will be used to process the data.

5.13 If you receive information about another person, even if you disclose it in a way intended to protect the individual's confidentiality, this does not necessarily mean that you can share this data with others. It is appropriate to discuss confidential issues with your Line Manager but only in a private setting, and this sharing is in line with the execution of your duties.

5.14 You should not discuss confidential matters relating to an individual with colleagues, or other agencies unless you have permission of the data subject, or this serves a legitimate purpose.

5.15 Be mindful when sharing confidential information appropriately, either in conversation, by telephone or in a public place; ensure that you cannot be overheard.

5.16 You are responsible for ensuring that people who do not need to see confidential information cannot do so, including any information on your computer device or screen. You should not leave notes or information about where they can be seen, and they must be securely destroyed once they have served their purpose.

5.17 Should you receive a request for information about an individual from someone either within or outside CHSS, please refer them to your Line Manager unless the individual has agreed to you sharing the information.

5.18 Where you have the authority to take data off-site, for example working from home or travelling between sites, you are responsible for ensuring all data, whether the data is held on your ICT equipment or in a manual file, is always protected from unauthorised access.

5.19 If you breach any aspect of this policy, this may be grounds for formal action. Where you seriously breach this policy, a potential sanction may be dismissal or withdrawal of the role you undertake.

5.20 The UK GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject. If you know or suspect a data breach has occurred, do not attempt to investigate the matter yourself. You should immediately either discuss it with your Line Manager for guidance or initiate the Data Protection Reporting Procedure for formal investigation to take place. The breach should also be reported to the DPO who will determine whether this is a reportable incident to the Information Commissioner. You should preserve all evidence relating to the potential Personal Data Breach. In addition, formal action may be taken against the individual as outlined at 3.19 above.

5.21 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

6. Lawfulness and fairness

6.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

6.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

6.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

a) the Data Subject has given his or her Consent;
b) the Processing is necessary for the performance of a contract with the Data Subject;
c) to meet our legal compliance obligations.;
d) to protect the Data Subject's vital interests; or
e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes

for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

6.4 Where necessary, you must identify and document the legal ground being relied on for each Processing activity.

Consent

6.5 A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

6.6 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.7 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.8 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

6.9 Where appropriate, you will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

Transparency (notifying data subjects)

6.10 The UK GDPR requires Data Controllers to provide detailed, specific

information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.11 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

6.12 When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

Purpose limitation

6.13 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.14 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

Data minimisation

6.15 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated

to your job duties.

6.16 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

6.17 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted.

Accuracy

6.18 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
You will ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Security of Data

6.19 You are responsible for ensuring that any personal data (on others) which is held is kept securely and is not disclosed to any unauthorised third party. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

6.20 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

6.21 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know

and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

6.22 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

6.23 You will ensure all personal data is accessible only to those who need to use it. This will be based upon the sensitivity and value of the information in question, but you should always consider keeping personal data:
- in a lockable room with controlled access.
- in a locked drawer or filing cabinet.
- if stored electronically/digitally, password protected, stored in a system which has MFA/2FA enabled and is encrypted.

6.24 You should ensure that display screens, laptops and handheld devices are not visible except to authorised staff and volunteers and that your ICT passwords are kept confidential. You should not leave devices unattended without locking the screen and manual records will not be left where they can be accessed by others.

6.25 Any device containing personal data must be encrypted.

6.26 Personal data should be retained according to your department/section's guidelines or disposed of in a way that protects the rights and privacy of the data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Storage limitation

6.27 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

6.28 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the

legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

6.29 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's procedures. This includes requiring third parties to delete such data where applicable.

6.30 Where necessary, you will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Transfer limitation

6.31 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

6.32 We do not currently transfer personal data outside the UK. We will amend this policy if the position changes.

Data Subject's Rights and Subject Access Requests (SAR)

6.33 If we hold personal data on an individual, they have the right to access the information, unless it is exempt under legislation.

6.34 Where we receive a SAR for information (this must be in writing, including email correspondence), we must respond without delay and, at the latest, within one month of receipt. You must verify the identity of an individual requesting data under any of the rights listed below (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation). You must immediately forward any Data Subject request you receive to the DPO.

6.35 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(i) be notified of a Personal Data Breach which is likely to result in f to their rights and freedoms;

(j) make a complaint to the supervisory authority; and

(k) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

6.36 Unlike previous legislation, we cannot charge for a request for information (SAR). Exceptions are detailed in Appendix 1.

6.37 Data portability requests will be handled in the same process.

The Right to Erasure

6.38 Data subjects have the right to ask us to erase their personal data. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.

6.39 Care and consideration should be given to any such request and the response may be dependent on the lawful basis under which the data was processed. There may be advantages to the data subject in suppressing, not deleting, their data and this may need to be explained to the data subject. You must immediately forward any request to erase

personal data to the DPO.

Safeguarding

6.40 Sensitive, personal information may need to be shared in the event of a safeguarding concern or incident. It is vital that any safeguarding information is shared appropriately and with confidentiality in mind.

6.41 Safeguarding information can always be shared internally within CHSS without the need for an individual's consent, and there are certain situations where this may need to be shared externally without consent, for example if there is immediate danger or if a crime has been committed. You must contact the DPO for advice before sharing any information externally.

6.42 In line with the CHSS Safeguarding Policy (Link), if you or another individual's safeguarding is of a concern:

- If you or the individual are in immediate danger, you should phone the Police or emergency social worker/agency, as appropriate.
- If you or the individual are in less immediate danger, you should record the information securely and inform your line manager and the Safeguarding Team as soon as possible.

6.43 It is important that safeguarding concerns and incidents are recorded securely and appropriately. When a safeguarding concern is raised, you should complete a Safeguarding Incident Form (Link). This may need to be provided to external agencies in the event of referral and may act as evidence in an investigation.

6.44 If you have handwritten notes from an initial disclosure or concern, keep these securely and confidentially, transfer the contents to a Safeguarding Incident Form as soon as possible then shred the original notes. These may act as evidence.

6.45 Safeguarding incidents will be recorded in a Safeguarding Case Tracker. This will be anonymised, kept confidential and used for monitoring and audit purposes.

Accountability

6.46 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Record keeping

6.47 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

6.48 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

Privacy By Design and Data Protection Impact Assessment (DPIA)

6.49 We are required to take account of privacy at all stages of our operations when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles (Privacy by Design).

6.50 Data controllers must also conduct DPIAs in respect to high risk Processing. We do not currently carry out any high-risk processing. We will amend this policy if the position changes.

Third Parties

6.51 We may from time to time use reputable third parties for the processing of data but we will not do so unless certain safeguards and contractual arrangements have been put in place.

6.52 You may only share the Personal Data we hold with another employee, agent or representative of our Company if the recipient has a job-related need to know the information.

6.53 You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and
- a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

Automated Processing (including profiling) and Automated Decision-Making

6.54 We do not currently envisage that any decisions will be taken about data subjects using automated means but will update this Data Protection Policy and associated privacy notices if this position changes.

Direct marketing

6.55 We are subject to certain rules and privacy laws when marketing to our customers.

6.56 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

6.57 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

6.58 A Data Subject's objection to direct marketing must be promptly honored. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Role of the People Driven Development Department

6.59 The People Driven Development Department includes the Director of People Driven Development, the Head of Volunteering and the Head of People. They are available, to support the Director of Finance & ICT to give advice and interpretation to you on any aspect of this policy.

7. Monitoring and Review

7.1 The Data Management Group, led by the Director of Finance & ICT, formed of representatives from each department, will discuss data protection and legislative updates on a regular basis. This group will monitor the effectiveness of this policy to ensure compliance with the UK GDPR.

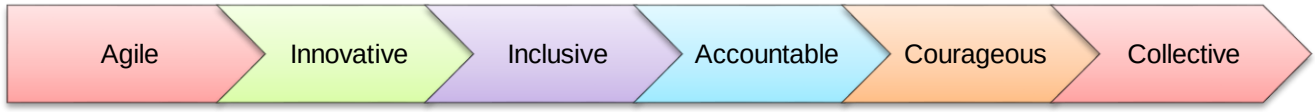
7.2 On an annual basis prior to re-registration with the Information Commissioner, the Director of Finance & ICT will provide each Director and Head of Service with a copy of CHSS's registration requesting that this be reviewed with any proposed amendments incorporated into the registration. The updated registration form will be submitted to the Executive Team (Directors) seeking their approval prior to submission to the Commissioner.

7.3 On an annual basis, details of the number of Subject Access Requests (SAR) and whether these access requests have been arranged within the time set out by the UK GDPR will be reported to the CHSS Board of Trustees.

7.4 This policy will be reviewed 3 years or earlier if deemed appropriate. If this policy is not reviewed within the above timescale, the latest approved policy will continue to apply.

8. Changes to this Data Protection Policy

8.1 We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy on 15 March 2022.



APPENDIX 1: Data Protection definitions

Child is “Any person below the age of 18 years. If the processing relates to the offering of information social services (social media) then the relevant age is 16. A lower age can be set by Member States by not less than 13.”

Data Controller: Chest Heart & Stroke Scotland is the data controller of all Personal Data relating to our Organisation Personnel and Personal Data used in our business for our own commercial purposes not an individual staff member. Data controllers must ensure that any processing of personal data for which they are responsible complies with the UK GDPR. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data Subject is the living, identified or identifiable individual whom personal data is about. The GPDR does not count as a data subject an individual who has died or who cannot be identified or distinguished from others (anonymised). Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Processor in relation to personal data, means any person (or system) who processes the data on behalf of the Data Controller.

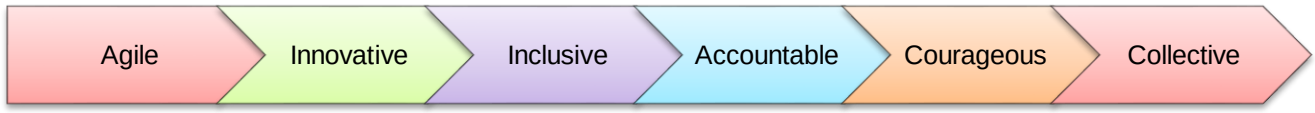
Data Protection Officer (DPO): the CHSS data protection manager with responsibility for data protection compliance.

Data is defined as information:

Stored in a form capable of being processed by computer (such as word-processor documents, spreadsheets, databases, emails, intranet or website content, social media content, phone contacts etc.).

Recorded in any form for later processing (such as paper-based forms, written notes, CCTV pictures). This also includes photos and video.

Stored as part of a 'relevant filing system.' Note that this definition is very broad and covers such things as card indexes and microfiche files as well as traditional paper-based files. It would be as well to assume that any paper-based data falls under the UK GDPR, including post-it notes, diaries and notebooks for example.



Data Portability: The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Data Protection Impact Assessment (DPIA) (also known as privacy impact assessment or PIA) is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. While not a legal requirement under the DPA, the Information Commissioners Office (ICO) has promoted the use of DPIAs as an integral part of taking a Privacy by Design approach.

Data Subject's Consent is "Any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed."

Relevant Filing System is defined as: "Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralised or dispersed on a functional or geographical basis"

Personal Data is any information relating to an (directly or indirectly) identified or identifiable natural person. Personal Data includes Sensitive Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach is "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether. Although this approach is

not a requirement of the Data Protection Act, it will help organisations comply with their obligations under the legislation. The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example, when:

1. building new IT systems for storing or accessing personal data.
2. developing legislation, policy or strategies that have privacy implications.
3. embarking on a data sharing initiative; or
4. using data for new purposes.

Processing is “Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction”.

Sensitive Personal Data means data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Special Categories of Data is “Personal data which is revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures.”

Genetic Data is “All data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development.”

Biometric Data is “Any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, or fingerprint identification.”

Data Concerning Health is “Any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual.”

Subject Access Request (SAR)

Under the UK GDPR, individuals will have the right to obtain:

1. confirmation that their data is being processed; and
2. access to their personal data; and
3. other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Requests must be processed without delay and at the latest within one month of receipt. Fees cannot be charged for a SAR. CHSS may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.