DATA PROTECTION POLICY

For all staff across the Percy Hedley Foundation

Policy Control/Monitoring

Version:	0.7
Approved by: **(Name/Position in Organisation)** **Date:**	**Director – Corporate Services** **November 2023**
Author of policy: **(Name/Position in organisation)**	Data Protection Officer
Date issued:	September 2017
Revision Cycle:	Every two years
Revised (Date):	November 2023
Target audience:	All Percy Hedley employees
Amendments/additions	January 2020 - Updated various sections to reflect DPIA and APD now in place, following updated Special Category Data Guidance from the ICO. April 2021 – Location of where policy held changed to PHF Connect, title of Role changed regarding Policy approval, Section 1.1: UK GDPR added, Section 2.4 updated, Section 16.2 updated to state two months if complex, Section 21: removal of reference to Brexit. Section 21.5: link added to ICO, Section 25: changes of euros to pounds and ICO terminology added, Section 28: Location changed to PHF Connect, Appendices numbered updated throughout. September 2021. - Update to take into account Privacy Shield/USA alternative data transfer arrangements and EU/UK current adequacy arrangements (see Section 21.1). Data Protection Lead added as a contact (Section 2.3)

Replaces/supersedes:	V0.1, V0.2, V0.3, V0.4, V0.5, V0.6
Associated Policies: **(insert hyperlinks)** **Associated National Guidance**	**The following policies can be accessed via the Foundation's PHF Connect:** • Privacy Notices • Subject Access Request Procedure • Appropriate Policy Document • Data Protection Impact Assessment (DPIA) Procedure • Foundation DPIA for processing Special Category Data • Processing Special Category Data Document • Data Breach Procedure • Data Retention Policy • Data Archive Procedure • Sensitive Data Procedure • Using Images of People and Consent Procedure • Recording Notes Best Practice Guidance • Records Management and Information Policy • CCTV Policy & Procedure • Fundraising Team's Direct Marketing Procedure And; • Disciplinary Policy • IT Acceptable Use Policy

	• Information Systems Policy
Document status	This document is controlled electronically and shall be deemed an uncontrolled documented if printed. The document can only be classed as 'Live' on the date of print.

Equality Impact Assessment

This document forms part of Percy Hedley's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.
As part of its development this document and its impact on equality has been analysed and no detriment identified.

Version Control Tracker

Version Number	Date	Author/ Title	Status	Comment/Reason for Issue/Approving Body
V0.1	September 2017	LGC - DPO	Archived	Mandatory requirement GDPR
V0.2	September 2018	LGC - DPO	Archived	Review
V0.3	September 2018	LGC - DPO	Archived	Review
V0.4	January	LGC - DPO	Approved/live	Review

Version Number	Date	Author/ Title	Status	Comment/Reason for Issue/Approving Body
	2020			
V0.5	April 2021	KM - DPO	Approved	Review
V0.6	Sept 2021	MGS - DPL	Approved	Review

Roles & Responsibilities

The following roles will have specific areas of responsibility for this policy:-

Role	Responsibility
Head of Service or Registered Manager	Ensuring implementation of compliance requirements across individual services.
Data Protection Officer	Monitoring compliance. Review and updates (where required) of this policy in accordance with any changes in regulations, law etc.
Director – Corporate Services	Final approval of any changes to this policy.

CONTENTS

1. Introduction

1.1 The Percy Hedley Foundation ("the Foundation") is committed to complying with privacy and data protection laws including the Data Protection Act 2018 ("the DPA") and the UK GDPR .(referred to as GDPR within the remainder of this policy) This policy sets out what we must do to protect individuals' personal information.

1.2 Anyone who handles personal data in any way on behalf of the Foundation must ensure that they comply with this policy. **Section 3** of this policy describes what comes within the definition of "personal data". Any breach of this policy will be taken seriously by the Foundation and may result in disciplinary action, up to and including dismissal. Serious action may also be taken by external sources. **Please refer to section 25, Offences, fines and liabilities under the regulation for more information.**

1.3 All staff will be made aware of Data Protection requirements and best practice of the Foundation by reading this mandatory document.

1.4 This policy will be reviewed annually and will be amended to reflect any future changes in legislation, regulatory guidance or internal policy decisions.

2. Scope

2.1 The types of personal information that we handle includes, but is not limited to, details of: Staff, Students, Service Users and Contractors.

2.2 This is an overarching policy for the Foundation.

2.3 The Foundation's Data Protection Officer (DPO) who is the first point of contact for compliance relating to Data Protection and this policy. Any questions or concerns can be raised directly to the Foundation's DPO or Data Protection Lead at dpo@percyhedley.org.uk. Alternatively, you can contact your line manager in your individual service area.

2.4 **The Foundation has a current ICO registration,** which can be viewed online via the public register on the website of the ICO (www.ico.org.uk).

3. Definitions of data protection terms

The following terms will be used in this policy and defined below:

3.1 **data subjects** include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.2 **personal data** means information relating to a living person who can be identified from that information (or from that information when combined with other information in our possession). Personal data can be factual (such as name, address or date of birth) or it can be an opinion (such as an appraisal). Personal data can be either paper based or electronic format (including emails).

3.3 **data controllers** are the people who, or organisations which, decide the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to process personal data in compliance with the DPA and GDPR. **The Foundation is the data controller of all personal data that we manage in connection with our work activities across our various services, across multiple sites.**

3.4 **data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website or server hosts, pension providers or other service providers which can handle personal data on our behalf.

3.5 **EEA** is the European Economic Area which includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.6 **ICO** means the Information Commissioner's Office (the authority which overseas data protection regulation in the UK).

3.7 **processing** is any activity that involves use of personal data. It includes obtaining, recording, holding, organising, amending, using, disclosing or destroying personal data.

3.8 The GDPR defines **special category data** as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;

- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

The main part of the Foundation's data processing is in relation to health. For further information on the data we process in relation to this processing, please refer to our **Special Category Data Processing Document.**

Genetic and biometric data have been added as new categories (the Foundation this time do not process either category).

Under the GDPR criminal records will be no longer be classified as special category data. Please see **section 23.5** for further information relating to criminal records.

3.9 **children's personal data** the GDPR contains new provisions intended to enhance the protection of children's personal data. The current age defined by the GDPR is anyone under the age of 16, however the UK have adopted defining the child age limit as anyone 13 years or under. Any vulnerable adult (regardless of age) will also be classed as child, for the purposes of data processing.

3.10 **other terms used in this policy:**

appropriate adult is the parent or guardian who will sign consent on behalf of a vulnerable individual (data subject).

vulnerable individual is a person in need of special care and support, due to disability (regardless of their age).

4. Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The principles (**sections 5 to 11**) are similar to those in the previous DPA 1998, with added detail at certain points and a new accountability requirement, which is the most significant addition, as requires we evidence **how** we comply.

The GDPR does not have principles relating to "individuals rights" and "overseas transfers of personal data" – these are specifically addressed in separate articles and are covered in **sections 12 to 21** of this policy.

In respect of any personal data that we deal with as a data controller, all Foundation employees are required to comply with these regulations (summarised in **sections 5 to 24** below).

Personal data must be:

4.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

4.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.4 accurate and, where necessary, kept up to date;

4.5 kept in a form which permits identification of data subjects and not kept longer than necessary;

4.6 processed in a manner that ensures appropriate security of the personal data; and

4.7 the controller shall be responsible for, and be able to demonstrate, compliance with all the above principles.

5. Processing data lawfully, fairly and transparently

5.1 The first principle requires that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals.

5.2 To do this, we must establish our **legal basis** before we can process personal data:

- **Consent** of the data subject
- Processing is necessary for the **performance of a contract** with the data subject or to take steps to enter into a contract.
- Processing is necessary for compliance with a **legal obligation**.
- Processing is necessary to protect the **vital interests** of a data subject or another person.
- Processing is necessary for the **performance of a task** carried out in the public interest or in the exercise of official authority vested in the controller.
- Necessary for the purposes of **legitimate interests** pursued by the controller or a third party, expect where such interests are overridden by the interests, rights or freedoms of the data subject.

Under the GDPR there are also **special categories of data** that also must be used for the purposes of processing in addition to the above. **Please see appendix 1 for further information.**

When processing any special category data organisations must also outline their **Schedule 1 Condition for Processing under the DPA 2018.**

The Foundation outline this is in our Processing Special Category Data Document as well as our Privacy Notices.

5.3 Legal grounds to process personal data in relation to *direct marketing* will either be **Legitimate Interest** *or* **Consent**. Please see the **Fundraising Team's Direct Marketing Procedure** for how they deal with direct marketing, and the Fundraising section of our Privacy Notice for wider legal bases for processing different categories of data.

Please note; any *direct marketing* must also comply with **Privacy and Electronic Communications Regulations** (**PECR**) https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

5.4 The Foundation has different legal ground for the processing of personal data, depending on which category of personal data we are processing. Our full legal bases for processing can be found in our **Privacy Notices**, as well as our **Processing Special Category Data Document**.

5.5 Every time we receive personal data about a person, which we intent to keep, we must provide the data subject (or appropriate adult) with our "fair processing information".

In other words we will tell them promptly:

- who will be holding their information, i.e. the Foundation and which specific service;
- our legal basis for the processing of their data;
- why we are collecting their information and what we intend to do with it, for instance, send them mailing updates relating to specific fundraising activities;
- how long we plan to hold their information for, in line with our services data retention procedures;
- if we plan to share their information with any other organisation we will outline who and for what purpose, and advise if that organisation is based outside the EEA. For instance, our schools and college may share information with Ofsted, based in the UK for the purposes of achievement rates.

We will do this via our **External Privacy Notice** which can be found in the footer of our external websites http://www.percyhedley.org.uk/privacy-notice-4/

An **Internal Employee Privacy Notice** is available on our internal intranet via Staff Room.

5.6 In service areas where CCTV is required for legitimate purposes, you must ensure the appropriate signage is displayed. Please refer to the Foundation's CCTV Policy & Procedure for further information.

Further guidance can also be found on the ICO website – https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

5.7 We will only engage in processing of personal data which comes within the categories set out in our Privacy Notice. Processing for additional purposes must not take place. The Privacy Notice is reviewed annually to ensure it is still accurate and up to date. If you think our Privacy Notice(s) is inaccurate or requires updating please contact our DPO.

6. Personal data shall be collected for specified, explicit and legitimate purposes

6.1 The second data protection principle requires that any personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

6.2 This means we must not collect personal data for one purpose and then use it for another, unless the second purpose is implicit.

6.3 If you wish to process data you already hold for a new purpose you must consider whether the new purpose is compatible with the original purpose for which the data was collected. If the new purpose is incompatible, you may only proceed if:

- you get the individuals consent ; or
- you are under a legal obligation to carry out the processing.

Please note; any further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall **not** be considered to be incompatible. However, if you wish to re-use the archive materials for another purpose e.g. an event, you must speak to the

Foundation's DPO in the first instance and we may need to seek further legal advice.

7. Personal data must be adequate, relevant and limited

7.1 The third data protection principle requires that any personal data we keep must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.2 This means we must only collect data that is needed for the purposes of processing, for instance, do not ask for more than is needed for the task e.g. you need ID to verify identity but ask for multiple ID's when 2 would have been sufficient.

8. Personal data must be accurate and, where necessary kept up to date

8.1 The fourth data protection principle requires that *any* personal data we keep must be accurate and, where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

8.2 This means we must ensure any inaccurate data we identify is immediately updated, or deleted to ensure an accurate and robust database, not only for the purposes of GDPR compliance but efficient working for both us and our customers and contractors.

8.3 This will also include images of data subjects, for instance photographs must be kept up to date and older photographs replaced where appropriate. Please refer to our **Using Images of People and Consent Procedure** for further guidance.

8.4 Services are required to have a suitable data cleansing procedures in place, to ensure that we regularly check our data, and adequately deleting/destroying/archiving as appropriate.

8.5 If you think that we are holding inaccurate data, please refer to our DPO or alternatively please contact your local line manager.

9. Data kept in a form which permits identification of data subjects and not kept longer than necessary

9.1 The fifth data protection principle requires that we must keep personal data 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.

9.2 This means that any personal data we hold (whether electronic or paper based) is stored in an easily identifiable format for identification purposes.

9.3 We are required to have a suitable data retention policy and procedures in place to ensure any personal data is clearly identifiable, securely archived and subsequently securely destroyed or fully erased from our systems where the data is no longer needed for the purposes we collected it for.

Please note; we can only archive personal data for regulatory, legal or specific business purposes. If not, then we cannot archive and the data must be immediately securely destroyed or fully erased from our systems.

9.4 Individual service areas across the Foundation may have different retention periods for disposing of personal data, depending on their regulatory requirements. For further guidance on this matter please refer to our **Data Retention Policy** and accompanying **Archiving Procedure**.

If you think that we are holding data that is no longer needed, please refer to our DPO or alternatively please contact your line manager.

Please note; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

10. Data shall be processed in a manner that ensures appropriate security of the personal data

10.1 The sixth data protection principle requires that we process all personal data in a manner that ensures appropriate security of that data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.2 We are required to put in place procedures and policies to keep personal data that we hold secure.

10.3 When we are dealing with Special Category Data (as defined in section 3.8), more rigorous measures are likely to be needed. The Foundation takes a risks based approach to this type of processing which is documented in our **DPIA for the processing of Special Category Data.**

10.4 The following security procedures must be followed in relation to all personal data processed by the Foundation:

- Any identifiable personal data (as defined in section 3.2) that needs to be transferred to a portable device must be encrypted, using IT approved encrypted memory sticks only.
- Work mobiles: any staff member issued with a work mobile will need to ensure they use the password pin at all times, they also must ensure the mobile device is only used for work purposes.
- Personal mobiles: all staff must ensure they do not access work information from their own personal devices e.g. sending and receiving emails, making and receiving calls and storing work contact details.
- Entry controls: Any stranger seen in an entry-controlled area must be reported.
- Emailing personal data: Any information relating to data subjects must only be sent from your work email (never use a personal email).
- Emailing to a personal account: You must never email work related information containing personal information or confidential/financial information etc. belonging to the Foundation from your work email account to your personal email account.
- If you are **emailing sensitive identifiable personal data** outside our network to any external third party you must be ensure the email is encrypted following our **Sensitive Data Procedure**.
- When emailing ***any*** information to multiple (**external**) recipients: you must ensure all recipients are blind cc'd into the email to ensure you do not disclose recipient's contact emails to the other recipients.
- Staff ID: Staff should ensure they wear their work issued ID badge and accompanying lanyards at all times when on Foundation premises, for further information please refer to our **Electronic Access to Buildings Policy.**
- Equipment: Users must ensure that individual monitors do not show confidential information to others who are unauthorised and that they log off (or lock) their PC or laptop when it is left unattended.
- Secure lockable desks and cupboards: Desks and cupboards must be kept locked if they hold confidential information of any kind (personal data is always considered confidential).
- Methods and disposal: Paper documents containing personal information must be disposed of via the Foundation's **Confidential Waste Bins**.

Memory sticks, CD-ROM's and other media on which personal data is stored must be physically destroyed when they are no longer required. This must be via a helpdesk task to IT.

- Backing up data: Daily back-ups must be taken of all data on our systems. Data must not be stored on local drives or removable media as these will not be backed up.
- Travelling with personal data and remote working staff: Staff must keep data secure when travelling or using it outside our offices.
- Secure exchange of data: Personal data must always be transferred in a secure manner. The degree of security will depend on the nature of the data; the more sensitive and confidential the data, the more stringent the security measures must be.
- Any payments made to the Foundation by credit card will be processed by appropriate staff in accordance with Payment Card Industry (PCI) Data Security Standard (DSS) compliance.

11. Governance and Accountability

11.1 The final principle, data protection principle seven requires the controller shall be responsible for, and be able to demonstrate, compliance with all the above principles (first to sixth).

11.2 We must ensure we maintain relevant documentation on all processing activities.

11.3 Individual service areas are responsible for ensuring their data compliance with data protection laws and regulations and this policy.

11.4 We must ensure we meet the principles of data protection by design and by default.

11.5 The Foundation's IT function will continue to regularly review and improve our security features on an ongoing basis in relation to data security.

11.6 The Foundation's Data Protection Officer will ensure implementation and continuous review of appropriate organisational measures to include a suite of Data Protection policies and procedures for use by the Foundation.

12. Individual Rights

12.1 The GDPR created some new rights for individuals and strengthens some of the rights that used to exist under the DPA 1998. Providing the following rights for individuals:

- The right to be informed

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

13. The right to be informed

13.1 The right to be informed encompasses our obligation to provide 'fair processing information', typically through our Privacy Notice. It emphasises the need for transparency over how we use personal data.

13.2 The information we supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in a clear and plain language, particularly if addressed to a child;
- free of charge

13.3 The information we supply is determined by whether or not we obtained the personal information directly from individuals. **Please see Appendix 2 for a table of information relating to this.**

14. The right of access

14.1 The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (first principle).

14.2 Details of how we deal with any Subject Access Requests (SARs) are outlined in our Privacy Notice.

14.3 Please see our internal **Subject Access Request Procedure** for full details of how we manage these.

14.4 Any requests for a SAR must be referred immediately to the Foundation's DPO.

15. The right to rectification

15.1 Individuals are entitled to have personal data rectified if inaccurate or incomplete (fourth principle).

15.2 If we receive such a request we must respond within one month so ensure our compliance with the GDPR. This can be extended to 2 months where the request for rectification is complex.

15.3 Where we decide not to take action in response to a request, we must explain why to the individual, informing them of their right to complain to the ICO.

15.4 If we have disclosed the personal data in question to any third parties, we must inform them of the rectification where possible. We must also inform the individual(s) about the third parties to whom the data has been disclosed where appropriate.

15.5 Any requests received regarding rectification must be referred immediately to the Foundation's DPO who will be responsible for managing with these requests.

16. The right to erasure

16.1 The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing (second principle).

16.2 If we receive such a request we must respond within one month to ensure our compliance with the GDPR.

You may extend the time limit by a further two months if the request is complex or if you receive a number of requests from the individual.

16.3 Where we decide not to take action in response to a request, we must explain why to the individual, informing them of their right to complain to the ICO.

16.4 If we have disclosed the personal data in question to any third parties, we must inform them of the deletion where possible. We must also inform the individual(s) about the third parties to whom the data has been disclosed where appropriate.

16.5 Any requests received regarding deletion must be referred immediately to the Foundation's DPO who will be responsible for managing with these requests.

17. The right to restrict processing

17.1 Under the DPA 1998, individuals had the right to 'block' or supress processing of personal data. The restriction of processing under the GDPR is similar.

17.2 When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.

17.3 Any requests received regarding deletion must be referred immediately to the Foundation's DPO who will be responsible for managing with these requests.

Please see Appendix 3 for further information of when this right applies.

18. The right to data portability

18.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purpose across different services.

18.2 Currently the Foundation does not have the IT infrastructure to be able to implement this requirement. We will keep this under regular review and take both a cost and risk based view.

18.3 We expect any such requests will be minimal (if at all) but any requests' are to be referred to the Foundation's DPO in the first instance who will liaise with the Foundation's IT Team accordingly.

19. The right to object

19.1 Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for the purposes of scientific/historical research and statistics.

19.2 Any requests received regarding deletion must be referred immediately to the Foundation's DPO who will be responsible for managing with these requests.

Please see Appendix 4 for further information relating to the right to object.

20. Rights related to automated decision making and profiling

20.1 The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

20.2 We do not currently automate the processing of any personal data and use this for profiling purposes without human intervention. This is due to the nature of the work conducted across the Foundation with vulnerable children and adults.

20.3 In circumstances where services within the Foundation do complete any profiling (with human intervention) we must have an appropriate process, and be able to evidence compliance with the GDPR. If anyone is planning any profiling please contact the Foundation's DPO prior to completing any profiling.

20.4 We have an ongoing legal obligation to monitor and identify whether any of our processing operations constitute automated decision making and update our procedures to deal with the requirements of the GDPR. If you identify an issue relating to a change in process that has, or may lead to an automated decision making and profiling you must immediately contact our DPO.

21. Transfer of data

As the Foundation do not currently transfer or receive personal data to Europe this has been deemed a low-risk area, however, we may deal with some third parties who do use servers based within the EU. This is covered by the current adequacy arrangement between the UK and EU.

21.1 **In most instances the Foundation and our third party providers only transfer personal data within the EEA, with the exception of Fundraising who use a third party provider (Mail Chimp) for marketing purposes. Their servers are located in the United States (US), therefore outside the EEA**. **Mail Chimp has in place appropriate safeguards in accordance with applicable legal requirements to provide adequate protection for any personal data transferred from Switzerland, the UK, or the EEA to the United States. For example, they use and have incorporated European Commission approved "Standard Contractual Clauses" or "Model Clauses" into their Data Processing Agreements.** https://mailchimp.com/legal/privacy/ **This information is transparent in our Privacy Notice.**

21.2 The GDPR imposes restrictions on the transfer of personal data outside the EEA, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

21.3 The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, as well as Norway, Iceland and Liechtenstein. This list may be updated.

21.4 As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation.

21.5 In instances where you determine that a personal data transfer outside the EEA is necessary, we need to ensure we are compliant with the conditions for transfer set out in the GDPR, therefore, you must immediately contact the Foundation's DPO as a DPIA will be required.

For further details:

https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/keep-data-flowing-from-the-eea-to-the-uk-interactive-tool/

22. Consent

22.1 Whilst consent is not required to process most data, it may be required to process some special category data (see **section 23**), and the Privacy and Electronic Communications Regulations (PECR) also makes it **mandatory** to gain an individual's consent if you wish to send **direct marketing electronically e.g. via email or text**.

For more information relating to PECR please see;
https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf

22.2 Under the GDPR it is clear that if your legal basis for processing personal data is consent then controllers must be able to demonstrate that consent was given.

22.3 Where our legal basis for the processing of personal data is consent, we must ensure the following;

- We are gaining some form of clear affirmative action, as silence, pre-ticked boxes or inactivity e.g. not responding to communications for example does not constitute consent.
- That we are keeping some form of record of how and when consent was given, as any consent must be verifiable (for both new clients and your existing client data base).

- We have procedures are in place to easily remove consent if and when requested, as individuals have the right to withdraw consent at any time.
- If processing for *electronic* marketing purposes, we are complying with not only GDPR requirements but also with PECR.

23. Processing sensitive (special category) personal data

23.1 Due to the nature of the Foundation's work, a large percentage of our personal data processing is defined by the GDPR as sensitive (special category) and rules apply to the processing of it. The categories of special category personal data are set out in the definitions in **section 3.8.**

23.2 Organisations that process any special category data are required under GDPR to have an Appropriate Policy Document (APD) outlining the processing of all special category data. **Please see our APD for further information on our processing.**

23.3 Organisations that process large volumes of special category data, classed as high risk processing are required to have a Data Protection impact Assessment (DPIA) for each category of special category data, outlining their technical and security safeguarding measures. **Please see our DPIA for the Processing of Health Information for further information.**

23.4 In most cases, in order to process special category data, due to the nature of the Foundation our legal basis for processing *most health data - is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care* (Article 9 (h) GDPR). **However, you should access our Privacy Notices and Processing Special Category Data Document as there may be some variation depending on the processing.**

23.5 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process special category data. If you are concerned that you are processing special category data and are not covered by our legal basis for processing in our Privacy Notice, or you are unable to obtain explicit consent for the processing, please speak to our DPO.

23.6 Purely financial information is not technically defined as special category data by the GDPR; however, particular care must be taken when processing such data, as the ICO is likely to treat a breach relating to financial data very seriously. In addition the Foundation will class financial data as confidential and therefore due care should be taken when processing.

23.7 Data relating to an individual's criminal record is no longer defined as special category data, but referenced separately in article 10 of the GDPR. Organisations are required to ensure appropriate technical and security measures are in place to safeguard this information and may be required to keep an official register **(please see section 4.3 of our APD for further information).**

As with financial information particular care must be taken when processing such data and any processing should only be done so in accordance with the first principle (see **section 5**).

24. Children

24.1 The Foundation currently does **not** target online services at children. However, in circumstances where the Foundation may introduce this as a service, the relevant service area must have an appropriate process, and be able to evidence compliance with the GDPR. Please contact the Foundation's DPO in advance of any implementation as a DPIA may be required.

24.2 If we were to ever offer any 'information society services' e.g. target online services at children, we need to ensure we must:

- obtain consent from a parent or guardian to process the child's data;
- the consent must be verifiable; and
- where any of our services are offered directly to a child (rather than an appropriate adult), we must ensure that our Privacy Notice is written in a clear, plain way that a child will understand.

25. Offences, fines and liability under the GDPR

Any offences of the DPA and GDPR could result in prosecution under section 55 by the ICO. A person must not knowingly or recklessly, without data controller consent:

- obtain or disclose personal data or the information contained in personal data, or;
- procure the disclosure to another person of the information contained in personal data.

This means Foundation employees can also be liable under section 55 and consequently may be fined directly by the ICO of up to £5,000.

Fines: The higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

26. Your responsibility

As an employee of the Foundation it is expected that you deal with all personal data in a confidential, sensitive and professional manner at all times.

Any Foundation employees that have access to individual records we hold on our employees and service users, for instance, medical files or HR files, are expected to access this information for **business purposes only and not further disclose the contents with any third party,** including service users and colleagues who are not privy to the information without prior appropriate authorisation.

This policy does not form part of any employee's contract of employment and we may amend it at any time, all staff are responsible for the success of this policy and should ensure that they take the time to read and understand it.

Employees who do not adhere to this policy may be subject to disciplinary action which may amount to dismissal for gross misconduct.

If you become aware an employee who is not abiding by this policy you should report this, in confidence, to the Data Protection Officer without delay.

A breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether our equipment or facilities are used for the purpose of committing the breach.

27. Data breaches

The GDPR has introduced a mandatory duty on all organisations to report certain data breaches to the ICO, and in some cases to individuals affected.

Please refer to our internal **Data Breach Procedure** for further information.

28. Associated Policies & References

Data Protection suite of policies and procedures

This policy should be read in conjunction with the following documents, available in the PHF Connect.

- Privacy Notices
- Subject Access Request Procedure
- Appropriate Policy Document
- Data Protection Impact Assessment (DPIA) Procedure
- Foundation DPIA for processing Special Category Data
- Processing Special Category Data Document
- Data Breach Procedure
- Data Retention Policy
- Data Archive Procedure
- Sensitive Data Procedure
- Using Images of People and Consent Procedure
- Recording Notes Best Practice Guidance
- Records Management and Information Policy
- CCTV Policy & Procedure
- Fundraising Team's Direct Marketing Procedure

Other related policies

This policy should be read in conjunction with Percy Hedley Foundation policies, such as, but not limited to:

- Disciplinary Policy
- IT Acceptable Use Policy
- Information Systems Policy

29. Monitoring and Compliance

Overall responsibility for the operation of the policy lies with the Head of Service or Registered Manager. The effectiveness of the policy will be formally reviewed and monitored by the Foundation's DPO, as a minimum on an annual basis to ensure that it continues to meet the requirements of The Foundation, the specific service areas and that it reflects best practice and statutory legislation as appropriate

Appendix 1

Continued from section 5.2 – **Additional conditions for special categories of data**

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Appendix 2

Continued from section 13 - **The Right to be informed**

The table below summaries the information we should supply to individuals and at what stage.

What information must be supplied?	**Data obtained directly from data subject**	**Data not obtained directly from data subject**
Identity and contact details of the controller and where applicable, the controller's representative and the Data Protection Officer	•	•
Purpose of the processing and the legal basis for the processing	•	•
The legitimate interests of the controller or third party, where applicable	•	•
Categories of personal data	•	•
Any recipient or categories of recipients of the personal data	•	•
Details of transfers to third country and safeguards	•	•
Retention period or criteria used to determine the retention period	•	•
The existence of each of data subject's rights	•	•
The right to withdraw consent at any time, where relevant	•	•
The right to lodge a complaint with a supervisory authority e.g. The ICO	•	•

The source the personal data originates from and whether it came from public accessible sources		•
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	•	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	•	•
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Appendix 3

Continued from section 17 - **The right to restrict processing**

We will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review your individual service area procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it involves disproportionate efforts to do so.

You must inform individuals when you decide to lift a restriction on processing.

Appendix 4

Continued from section 19 - **The right to object**

When we process any personal data for the performance of a legal task or the Foundation's legitimate interests

Individuals must have an objection on "grounds relating to his or her particular situation".

We must stop processing the personal data unless:

- we can demonstrate compelling legal grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We must inform individuals of their right to object "at the point of first communication" as well as this being outlined in our Privacy Notice.

This must be "explicitly brought to the attention of the data subject and shall be present and clearly and separately from any other information.

When we process personal data for direct marketing purposes

We must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no an exemptions or grounds to refuse.

We must deal with an objection to processing for direct marketing at any time and free of charge.

We must inform individuals of their right to object "at the point of first communication" as well as this being outlined in our Privacy Notice.

This must be "explicitly brought to the attention of the data subject and shall be present and clearly and separately from any other information.

If in the future we process personal data for research purposes

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If we conduct research where processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

For our processing activities that fall into any of the above categories and are carried out online, we will give an opt-out option.