

# Data Protection Policy & Guidelines

DOCUMENT CONTROL		
		Date
<b>Developed by:</b>	Chris Traynor & Sheila O'Flynn (Freedom of Information & Data Protection Officer)	April 2019
<b>Approved by:</b>	Leadership Team	
<b>Authorised by:</b>	Seán Abbott Chief Executive	April 2019
<b>Circulation Date this version:</b>	Printed: Electronic:	January 2022
<b>Review By &amp; Date:</b>	Sheila O'Flynn Data Protection Officer	April 2022
DOCUMENT REVIEW HISTORY		
<b>Document Amended Y/N</b>	Yes	
<b>Version Number:</b>	5	

This is a controlled document: While this document may be printed the electronic version posted on the website is the controlled copy. Any copy can only be guaranteed for 24 hours after downloading.

<b>CONTENTS</b>		<b>Page</b>
<b>PART 1: Policy Introduction</b>		
1.1	The Six Data Protection Principles	3
1.2	Policy Statement	3
1.3	Policy Purpose	4
1.4	Policy Scope	4
1.5	Definitions/ Descriptions	4-5
<b>PART 2: General Guidelines</b>		
2.1	Introduction to Data Protection Principles	6
2.2	Lawful, Fair & Transparent Processing of Data	6
2.2.1	Lawful Processing	6
2.2.2	Fair & Transparent Processing	7
2.2.3	Special Category (Sensitive) Data & Fair Processing	7
2.3	Purpose Limitation	7
2.3.1	Who May Access Person Data	8
2.3.2	Permitted Disclosures of Personal Data	8
2.4	Data Minimisation	9
2.5	Storage Limitation	9
2.6	Accuracy	10
2.7	Integrity & Confidentiality (Security)	10-11
2.8	Rights of Data Subjects	11
2.8.1	Right to request a copy of Personal Data	11-12
2.8.2	Other Rights under the Data Protection Act	12
<b>PART 3: Risk Management</b>		
3.1	Introduction	13
3.2	Data Privacy Audits	13
3.3	External Compliance	14
3.4	Data Privacy Impact Assessments	14
<b>PART 4: Data Breach Management</b>		
4.1	Introduction	15
4.2	Management of a Data Breach in Cope Foundation	15
4.2.1	Incident Details	15
4.2.2	Notification of Data Breach and Risk Assessment	16-17
4.2.3	Evaluation & Response	17
<b>PART 5: Awareness Training &amp; Support for Staff who Process Personal Data</b>		
5.1	Introduction	17
5.2	Data Protection Awareness Training	17
5.3	Data Protection Support	17
5.4	Review	17
<b>Appendix 1</b>	<b>Processing the Data of People we Support for Medical</b>	<b>18</b>

	Purposes	
<b>Appendix 2</b>	Guidance on collection, purpose and storage of Photography & Video Consent Form & Guidance	19-20
<b>Appendix 3</b>	Photographs or Video/Audio Recordings of People we Support	22-23
<b>Appendix 4</b>	Access Request Form	24
<b>Appendix 5</b>	Access Request Form – Staff Guidance	25
<b>Appendix 6</b>	Data Privacy Notice	26
<b>Appendix 7</b>	Short Privacy Statement– When Collecting Data	27
<b>Appendix 8</b>	Rights of Data Subjects - Leaflet	28

## **PART 1: Policy**

### **1.1 The Six Data Protection Principles**

Under the Data Protection Acts 1988 to 2018 Cope Foundation as a Data Controller has a legal responsibility to ensure personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (*'lawfulness, fairness and transparency'*)
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (*'purpose limitation'*)
3. Adequate, relevant and limited to what is necessary (*'data minimisation'*)
4. Accurate and where necessary kept up to date (*'accuracy'*)
5. Kept for no longer than is necessary for the purposes for which the data are processed (*'storage limitation'*)
6. Processed in a manner that ensures appropriate security, integrity and confidentiality of the data (*'integrity & confidentiality'*)

**Cope Foundation shall be responsible for and able to demonstrate compliance with all the principles above. (*'accountability'*)**

### **1.2 Policy Statement**

Cope Foundation as a 'Data Controller' shall endeavour:

- To comply with both the Data Protection Acts and in particular the six Data Protection principles and good practice;
- To protect the privacy rights of the people we support and the staff of Cope Foundation in accordance with Data Protection legislation;
- To ensure that Personal Data in Cope Foundation's possession is kept safe and secure;
- To support staff to meet their responsibilities under the Data Protection Principles and the overall principle of accountability;
- To respect individuals' rights;
- To provide awareness training and support for staff that process Personal Data.

### 1.3 Policy Purposes

The purposes of this Data Protection Policy are:

- To outline how Cope Foundation endeavours to comply with the Data Protection Acts;
- To provide good practice guidelines for staff;
- To protect Cope Foundation from the consequences of a breach of its responsibilities.

### 1.4 Policy Scope

- This Policy applies to all staff who process Personal Data of the people we support and/or staff.

### 1.5 Definitions/ Descriptions

**'Access Request'** is where a person makes a request in writing or in person to an organisation for the disclosure of their Personal Data, under section 91 of the Data Protection Acts. (**Appendix 4** Access Request Form)

**'Data'** is information in a form that can be processed. It includes automated or electronic Data (any information on computer or information recorded with the intention of putting it on computer) and manual Data (information that is recorded as part of a *Relevant Filing System*, or with the intention that it should form part of a *Relevant Filing System*).

**'Data Controller'** is a person who (either alone or with others) controls the contents and use of Personal Data. (Cope Foundation as a 'legal person' is a Data Controller).

**'Data Processing'** is the performance of any operation or set of operations on data, including:

- Obtaining, recording or keeping the Data;
- Collecting, organising, storing, altering or adapting the Data;
- Retrieving, consulting or using the Data;
- Disclosing the Data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the Data.

**'Data Processor'** is a person who processes personal information (Data) on behalf of a Data Controller, but does not include an employee of a Data Controller who processes such Data in the course of his/her employment; for example, this might mean an employee of an organisation to which the Data Controller out-sources work. The Data Protection Acts places responsibilities on such entities in relation to their processing of the Data.

**'Data Subject'** is an individual who is the subject of Personal Data.

**'Personal Data'** is Data relating to a *living* individual who is or can be identified, either from the Data or from the Data in conjunction with other information, which is in, or is likely to come into the possession of the Data Controller. It includes information in the form of photographs, audio and video recordings, and text messages.

**'Relevant Filing System'** is any set of information organised by name, date of birth, PPSN, payroll number, employee number, or any other unique identifier.

**'Special Category Personal Data' (Sensitive data)** relates to specific categories of Data which are defined as Data relating to a person's race; ethnic origin, politics, religion or other beliefs; trade union membership, genetics, biometrics (where used for ID purposes) health, sex life or sexual orientation. There are separate and specific safeguards for personal data relating to criminal offences and convictions.

**The Data Protection Acts** Data Protection Acts 1988 to 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling Personal Data.

## **PART 2: General Guidelines**

### **2.1 Introduction to Data Protection Principles**

The Data Protection Acts confer rights on individuals, as well as placing responsibilities on those persons processing Personal Data. Cope Foundation, as a Data Controller, endeavours to meet its legal responsibilities in relation to the information it processes. This involves the obligation on all staff involved in processing Personal Data to apply the Six Data Protection Principles, in order to safeguard the privacy rights of individuals.

Cope shall be responsible for and able to demonstrate compliance with the six Data Principles of:

- Lawfulness, Fairness, Transparency.
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity & Confidentiality (Security)

### **2.2 Lawful, Fair and Transparent Processing of Data**

#### **2.2.1 Lawful Processing,**

To process data lawfully it must have been fairly obtained **and** the processing must have a legal basis.

The legal bases which Cope, depending on the circumstances, may rely on include:

- When it is necessary to perform a contract or to take steps at the person's request (clearly with their knowledge and consent) before entering into a contract, such as a contract to provide services, or an employment contract;
- When it is necessary for Cope Foundation to comply with a legal obligation, such as reporting to a statutory or regulatory body. e.g. HIQA, Túsla, or law enforcement;
- When it is necessary to protect a person's vital interests in exceptional circumstances, such as in a case of a medical emergency;
- When it is necessary for the legitimate interests of Cope Foundation, except where those interests are overridden by your interests or your fundamental rights and freedoms. An example of Cope's legitimate interest would be where we gather and process information in our endeavour to monitor and optimise our services to the people we support.
- OR
  - The Data Subject must have given consent to the processing for the specific purpose or purposes.

### **2.2.2 Fair & Transparent Processing**

The Foundation will endeavour not process data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. To obtain information fairly and transparently Cope Foundation will at the time personal data is collected make the person or their representatives aware of:

- The Foundation's Short Privacy Statement (**Appendix 7**)
- The Foundation's Full Privacy Statement which is available on the home page of the Cope website under "Privacy Statement"
- The Foundation's Data Privacy Notice (**Appendix 6**) shall be displayed in offices, and on all public and service users' notice boards.

### **2.2.3 Special Category ('Sensitive) Data & Fair Processing**

**To fairly process special category ('sensitive') data it must be fairly obtained and one of these further conditions must be met, the processing must be necessary:**

- For legal claims or judicial purposes
- For employment, social security and social protection law
- In the Vital interests of the Data subject
- For the legitimate activities of a body with a political, philosophical, religious or trade union aim
- For reasons of substantial public interest
- Relating to personal data that is manifestly public
- For the purposes of preventive or occupational medicine
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- Public interest in the area of public health
- Explicit consent has been given

### **2.3 Purpose Limitation**

**To collect data for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;**

Cope endeavours to process Personal Data only in ways compatible with the purpose for which it was given initially. To comply with this rule, staff that process Personal Data should be aware:

- That a person should know the specific reason/s why information is being collected and retained;
- That the purpose for which the information is being collected is a lawful one;
- They are aware of the different categories of Data which are held and the specific purpose for each.
- That they do not further process data in ways that may be considered incompatible with the purpose for which the data was given or collected.
- Personal Data should only be used and disclosed in ways that are necessary or compatible with the original purpose for which it was obtained;
- Staff are not to disclose any Personal Data to any third party without consent of the Data Subject (see Permitted Disclosures of Personal Data below);



- Personal information should not be disclosed to work colleagues unless they have a legitimate interest in the Data in order to fulfil official employment duties.

### **2.3.1 Who may access personal Data?**

Access to personal data is strictly on a need-to-know basis. Unless there is another legal basis, unambiguous consent will be sought before any third party is authorised to access it. Those authorised to access personal data will vary, depending on whether you are a person supported by Cope Foundation or a family/guardian, a staff member or volunteer, or a person contracted for services.

We require third parties to respect the security of your data and to treat it in accordance with the law.

All our third-party service providers are required to take appropriate security measures to protect your personal data. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### **2.3.2 Permitted Disclosures of Personal Data:**

Personal Data may be disclosed without the express written consent of the Data Subject in the following circumstances:

- Where the Data Subject has already been made aware of the person/organisation to whom the Data may be disclosed. Third parties who may be provided access to personal data include the following:
  - Cope Foundation administration staff;
  - Cope Foundation healthcare professionals, including social workers, therapists, nurses, psychologists;
  - External healthcare professionals, including physicians and psychiatrists;
  - Staff/ Volunteers providing support to clients;
  - Statutory and regulatory bodies;
  - Banks, financial institutions, insurers, pension fund administrators;
  - Cope Foundation's legal advisors, as and when appropriate.

For further information see: <https://www.cope-foundation.ie/Privacy-Statement> & **Appendix 7** Short Privacy Statement.

- Where it is required by law;
- Where it is required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- Where it is required urgently to prevent injury or damage to health,

## **2.4 Data Minimisation**

### **Data collected should be adequate, relevant and limited to what is necessary**

- Only information necessary for the stated purpose should be collected, nothing more.
- Annual Data Privacy audits carried out by managers and their staff team will examine the relevance of the Personal Data sought from Data Subjects, through the various channels by which information is collected i.e. check to confirm that questions asked on forms are appropriate, etc.
- Annual Data Privacy audits - the audit should review any Personal Data already held, to make sure it is adequate, relevant and not excessive for the purpose for which it was collected.

## **2.5 Storage Limitation**

### **Cope Foundation will retain personal data for no longer than is necessary for the specified purpose or purposes**

- Staff are to be clear about the length of time that Data will be kept and the reason why the information is being retained;
- Generally, Personal Data collected for one purpose, should not be retained once that purpose has ceased;
- Exceptions may apply from specific legislation which require information to be retained for particular periods;
- Staff should refer to Cope Foundations Records Management Policy 2017 which includes time factors for the retention and destruction of data in manual and electronic form is to be adhered to;
- Annual Data Privacy audits should be undertaken to ensure storage limitation protocols are implemented. Carrying out this exercise will help identify where immediate remedial actions are required in order to be compliant with the GDPR.
- Personal Data, when no longer required, should be disposed of securely and where appropriate recorded using the centres data destruction register. The disposal method should be appropriate to the sensitivity of the Data. Shredding or incineration is appropriate in respect of Manual Data; and reformatting or overwriting in the case of Electronic Data;
- Particular care is to be taken when PC's or laptops are transferred from one person to another, or when being disposed of.
- Data Privacy Audits should be conducted and recorded using the Foundation's Data Privacy Audit tool (2019) with the support of the Data Protection Officer. (See – 3.1 Data Privacy Audit, p13).

## 2.6 Accuracy

### **Cope shall endeavour to ensure the data we process shall be accurate and where necessary kept up to date**

Cope Foundation endeavours to meet its duty of care to the people we support and to staff by maintaining records of personal information which are accurate, complete and up-to-date. In addition, it is in the interests of Cope Foundation to ensure that accurate Data is maintained for reasons of efficiency and effective decision making.

Therefore, it is important that:

- Manual and computer procedures are adequate to maintain high levels of Data accuracy;
- Staff should regularly audit their files to ensure that information is accurate and up to date;
- Appropriate procedures are in place, including periodic review and audit by managers, to ensure that Data is kept up-to-date;
  - Procedures are in place to ensure personal Data is accurate, including reviewing of records by managers on a regular basis;

Where a Data Subject informs or advises of any errors or changes to their Data, that it is amended accordingly, and as soon as reasonably possible.

## 2.7 Integrity & Confidentiality (security)

### **Cope shall endeavour to process data in a manner that ensures the security, integrity and confidentiality of the data**

Cope Foundation promotes high standards of security for **all** Personal Data. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the Data in question. Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of the Data and against their accidental loss or destruction.

Cope Foundation's standards of security include the following:

- Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractors;
- Access to any Personal Data within Cope Foundation is restricted to authorised staff for legitimate purposes only;
- Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information;
- Non-disclosure of personal security passwords to any other individual (including other employees in Cope Foundation);
- Information on computer screens and manual files to be kept out of sight from callers to our offices;

- Back-up procedures in operation for information held on computer servers, including off-site back-up;
- Personal Manual Data is to be held securely in locked cabinets, locked rooms, or rooms with limited access;
- Special care (including encryption) must be taken where mobile computing (including the electronic transfer of Personal Data via e-mail) and storage devices, such as laptops or other devices are used;
- Personal Data is not to be stored on portable devices except in essential circumstances. Where deemed essential, the Data (the device) must be encrypted. Arrangements are to be in place to fully delete the Data on the portable device when it is no longer being used;
- All reasonable measures are to be taken to ensure that staff are made aware of Cope Foundation's security measures, and comply with them;
- All waste papers, printouts etcetera to be disposed of appropriately.

## 2.8 Rights of Data Subjects

**Under the Data Protection Acts, data subjects have a:**

- Right to have any inaccurate information rectified or erased;
- Right to have Personal Data taken off a mailing list;
- Right to complain to the Data Protection Commissioner
- Right to Request a copy of Personal Data

### 2.8.1 Right to request a copy of Personal Data

Cope Foundation endeavours to provide access to personal data on request through Administrative Access (**Appendix 8** Rights of Data Subjects (leaflet); **Appendix 5** Access to Records Procedure). If data cannot be released through Administrative Access an individual person may apply either in writing (which may be via email) or make a verbal request.

Staff should be aware that verification of identity (Date of Birth & address/or telephone number) is needed to help identify the person and locate the information kept about him/her.

- The Subject Access Request form (**Appendix 4**) may be used by staff to record a verbal request. Requests under the Data Protection Act do not have to be made in writing.
- Any request from a third party or a solicitor should be forwarded without delay to The Data Protection Officer.
- Requests made under the Data Protection Act should be sent without delay to the Data Protection Officer

On making a request (in writing or in person) under the Data Protection Acts, any individual about whom an organisation, including Cope Foundation, keeps personal information on computer, or in a Relevant Filing System, is entitled within one month to:

- Know the purpose(s) for processing his/her Data;
- Know the identity of any third parties to whom the Foundation discloses the Data;
- Know the source of the Data, unless this would be contrary to public interest;
- Be informed of the logic involved in processing the Data, where the processing by automatic means of the Data has/is likely to constitute, the sole basis for any decision significantly affecting him/her;
- A copy of the Data being kept about him/her;
- Receive a copy of any Data held in the form of opinions expressed about the individual, except where such opinions were given in confidence;
- Clearly outlined reasons for an access refusal.

### **2.8.3. Other rights under the Data Protection Acts:**

- Right to have any inaccurate information rectified or erased;
- Right to have Personal Data taken off a mailing list;
- Right to complain to the Data Protection Commissioner.

The Rights of Data **S**ubjects Leaflet (**Appendix 8**) should be offered to any data subject who enquires about record rectification, erasure or how to stop data being processed.

## **PART 3: Risk Management**

### **3.1 Introduction**

There are three parts to data privacy risk management:

- Achieving Internal Compliance by conducting Data Privacy Audits
- Achieving external compliance with the Office of the Data Protection Commissioner
- Conducting Data Privacy Impact Assessments as required

### **3.2 Data Privacy Audits**

The principle purpose of an Internal Data Privacy Audit is to ascertain whether Cope Foundation is operating in accordance with the Data Protection Acts, and to identify any risks or possible contraventions of the legislation;

- Annual Internal Compliance Audits shall be undertaken by Managers in order to identify existing and potential risks;
- The Internal Compliance Audit will review both manual and electronic data procedures and compliance;
- The results will be recorded. A copy will be held by the centre and a copy will be forwarded to the Data Protection Officer. The audit's purpose is, in detail:
  - To list the categories of personal data held or processed by this Unit / Office / Functional Area
  - To set out the security measures, practices and controls to be applied for each category of personal data listed.
  - To guide Cope staff, contractors, volunteers etc. as to their responsibilities when handling, processing or interacting with the personal data listed in any way.
  - To demonstrate compliance with GDPR to the Office of the Data Protection Commission.
  - An interactive data privacy audit tool is available. Guidance and training on its use is provided on request by the Data Protection Officer.
  - All data privacy challenges that arise from the audit should be raised with the Data Protection Officer.
  - For guidance on conducting the internal Data Privacy Audit and to see examples of some typical categories of personal data found in a care setting, please request from the Data Protection Officer the document entitled 'Guide to preparing and using the Cope Foundation DPSA'.
  - The record of the audit must be lodged with the Data Protection Officer to be available for inspection by the Data Protection Commissioner.

The following templates are available from the Data Protection Office to support the outcomes of the data privacy audit:

- Records Retention Schedule & Guidance
- Records Destruction Log & Guidance.

### 3.3 External Compliance

All aspects of Data protection within Cope Foundation are subject to external audit which may be conducted on a periodic basis by the Office of the Data Protection Commissioner. Staff should be aware:

- Cope Foundation is accountable under the Data Protection Act 2018 and may be audited for its compliance with all aspects of this policy and the Data Protection Act 2018.
- Cope Foundation's Internal Data Privacy Audit records (above) are subject to audit by the Office of the Data Protection Commission.
- Cope Foundation's Data Breach records are subject to audit by the Office of the Data Protection Commissioner.
- Cope Foundation's Data Privacy Impact Assessment records (See 3.4) are subject to audit by the Office of the Data Protection Commissioner.

### 3.4 Data Privacy Impact Assessments

Data Privacy Impact Assessments can be used to identify and manage against any data protection risks arising from a new project which may affect the organisation or the individuals the organisation engages with.

Data Privacy Impact Assessments are mandatory in certain circumstances; among other things when:

- Implementing new technology to process data
- Sensitive personal data is being processed
- Data subjects are vulnerable
- Large amounts of data are being processed
- Using information to evaluate or profile individuals
- Implementing new monitoring or surveillance or testing procedures
- Sharing personal data with high risk countries
- Restricting the rights of individuals

Cope Foundation's Data Privacy Impact Assessment form is available on WorkVivo (Documents/GDPR area) or [here](#).

If a data privacy risk has been identified the advice of the data protection officer should be sought.

## **PART 4: Data Breach Management**

### **4.1 Introduction**

A Data breach may happen for a number of reasons, including:

- Loss or theft of equipment on which Data is stored;
- Inappropriate access controls allowing unauthorised use or sharing;
- Equipment failure;
- Human error e.g. misaddressing an email or postal address, or entering a wrong phone number for a facsimile;
- Unforeseen circumstances such as a flood or fire;
- Computer hacking;
- Access where information is obtained by deception (e.g. 'social engineering' where a person in conversation, extracts confidential information from another, without having an entitlement to that information).

### **4.2 Management of a Data Breach in Cope Foundation**

There are three elements to managing a Data breach:

1. Incident Details;
2. Notification of Data Breach & Risk Assessment;
3. Evaluation and Response.

#### **4.2.1 Incident Details**

Details of the incident should be recorded accurately by the Line Manager, including:

- Description of the incident;
- Date and time of the incident;
- Date and time it was detected;
- Who reported the incident and to whom it was reported;
- The type of Data involved and how sensitive it is;
- The number of individuals affected by the breach;
- Was the Data encrypted?
- Details of any Information Technology (IT) systems involved;
- Corroborating material.



## 4.2.2 Notification of Data Breach & Risk Assessment

### Internal Notification

- A Data breach must be reported within 24 hours or without delay by staff to their Line Manager, who in turn will immediately notify the Divisional Head and the FOI/Data Protection Officer with the Incident Details.
- The Manager, Divisional Head and the FOI/Data Protection Officer, and any other member of staff considered appropriate, will meet to assess the incident details and the risks involved, including:
  1. What type of Data is involved?
  2. How sensitive is the Data involved?
  3. How many individuals' Personal Data are affected by the breach?
  4. Were there protections in place e.g. encryption?
  5. What are the potential adverse consequences for individuals and how serious or substantial are they likely to be?
  6. How likely is it that adverse consequences will materialize?

### External Notification

- It is best practice to inform the Office of the Data Protection Commissioner (ODPC) immediately as part of the Foundation's response. (This allows the ODPC to advise the Foundation, at an early stage, on how best to deal with the aftermath of a Data breach, and also to ensure that there is no repetition. It also allows the ODPC to reassure those who may be affected by a Data breach that the ODPC is aware of it and that Cope Foundation is taking the issue seriously).
- Initial contact with the ODPC should be within two working days of becoming aware of the data breach incident. This initial contact may be by completing the breach notification form at <https://forms.dataprotection.ie/breach-notification> or by telephone. The FOI/Data Protection Officer will be responsible for reporting the breach or contacting the ODPC for advice.
- Depending on the nature of the incident, the ODPC may investigate the circumstances surrounding the data breach.
- Cope Foundation will also consider notifying third parties, such as An Garda Síochána, HSE, banks, who may be able to assist in reducing any adverse consequences for the data subject/s.
- Cope Foundation will notify individuals "where the breach is likely to result in a high risk to data subjects".(Guidance Note: A Quick Guide to GDPR Notifications. DPC. August 2019)
- The risk/impact to individuals will be assessed in line with Cope Foundation Risk Impact matrix. (Safety Statement Part 3: Site Specific Risk Register 2018. Cope Foundation. )
- When notifying individuals, Cope Foundation will consider the most appropriate medium for doing so. It will bear in mind the security of the medium for notification and the urgency of the situation. Specific and clear advice will be given to individuals affected by the Data breach, on the steps they can take to protect themselves and, what Cope Foundation is willing to do in order to assist them. Cope Foundation will also provide a contact person for further or on-going information.

- The DBMT will also consider notifying third parties, such as An Garda Síochána, bank or credit companies who can assist in reducing the adverse consequences to the Data Subject.

#### **4.2.3 Evaluation & Response**

Subsequent to any data/information security breach, a thorough review of the incident will be made by Cope Foundation. The purpose of this review will be to:

- Ensure that the steps taken during the incident were appropriate;
- Describe and record the measures being taken to prevent a repetition of the incident;
- Identify areas that may need to be improved;
- Document any recommended changes to policy and/or procedures which are to be implemented as soon as possible thereafter.

### **PART 5: Awareness Training & Support for Staff who process Personal Data**

#### **5.1 Introduction**

- Cope Foundation endeavours to support staff members who process Personal Data, through Data Protection Awareness Training and Data Protection Support mechanisms.

#### **5.2 Data Protection Awareness Training**

- Data Protection Awareness Training will take place during Induction of new staff, and at various intervals throughout an employee's professional career in Cope Foundation.

#### **5.3 Data Protection Support**

- Data Protection Support is provided by the FOI/Data Protection Officer.

#### **5.4 Review**

- This Policy will be reviewed every three years or earlier if appropriate, to ensure it remains comprehensive, current with legislation, and relevant to good practice.

## **APPENDIX 1- Processing the Data of People we Support for Medical Purposes**

### **A. DATA/INFORMATION**

Includes photographs, video/ audio recordings for 'medical purposes' (see "D" below).

### **B. IS CONSENT REQUIRED?**

Consent is not required where the processing of Data/ information is necessary for 'medical purposes', and is undertaken by:

- A Health Professional, or
- A person who in the circumstances owes a duty of confidentiality to the Data Subject that is equivalent to that which would exist if that person were a Health Professional.

### **C. HEALTH PROFESSIONAL**

- A Health Professional means a person who is a medical practitioner, a dentist, optician, pharmaceutical chemist, nurse or midwife, chiropodist, dietician, occupational therapist, orthoptist, physiotherapist, psychologist, child psychotherapist, or speech and language therapist (s.3(a) (b) Statutory Instrument 82/1989 – Data Protection (Access Modification) (Health) Regulations, 1989).

### **D. MEDICAL PURPOSES**

- The definition of 'Medical Purposes' includes for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of medical care, treatment or social care, for the management of health or social care systems and services, or pursuant to a contract with a health practitioner.

### **E. IMPLIED CONSENT**

- Consent may be implied, where the Data Subject provides information that will be recorded by a Health Professional or a person who owes an equal duty of confidentiality to the Data Subject, and the recording is for the purposes of preventive medicine, medical diagnosis, medical research (Data needs to be anonymised) the provision of care and treatment, and the management of health care services.
- The Data Subject should be informed of the reasons why the Data will be recorded, with whom it may be shared, and the length of time it will be kept.

**Reference:** Data Protection Act 1988 to 2018.s 52(1) & 52(2)

## **APPENDIX 2 - Guidance on the collection, purpose and storage of Photographs or Video/Audio Recordings of People we Support**

### **1. Consent to Photographs/Video/Audio Recordings (see Appendix 3)**

- Any photograph, video or audio recording of a person constitutes their Personal Data and is therefore, subject to the provisions of the Data Protection Acts.
- The people we support, their parents/guardians/advocates are permitted to take photographs or make video/audio recordings for their own personal use, for example at concerts or award events etc.

### **2. Recommended Good Practice**

- This good practice guidance is aimed at those who work in Units, Centres schools of Cope Foundation;
- Photos/Video Recordings taken for Medical, Social Care, Educational Events, Identification purposes do not require signed consent; where such photos are photos/video recordings are taken in order to provide a service or are required by legislation.
- Photos/video Recordings taken to celebrate individual or group events (e.g. a party, in a home, an outing or activity) do not require signed consent.
- If at a later date, photos taken for a private celebration are to be used for public purposes (e.g. Cope foundation publicity) consent must then be sought.
- Photographs, video/ audio recordings taken purely for personal use are exempt from the Data Protection Acts.
- Photos taken by a photographer from a local newspaper e.g. at an awards ceremony for the people we support. As long as the photographer has been given permission to do so by Cope Foundation, and the person we support and or their families/ guardians are aware that photographs of those attending the ceremony may appear in the newspaper, and they have not objected, this will then not breach the Data Protection Acts.
- When taking a photo(s)
  - Be sensitive to the person's preferences
  - Let the person know the purposes of the photo/video recording, who will have access to it, where it will be stored and how long it will be kept.

### 3. Security, Purpose Limitation, Storage Limitation

- Staff must not use their personal mobile devices to take photos/videos of people we support.
- Photos taken on a Cope Foundation mobile device should be transferred as soon as possible to the Cope Foundation network and should then be deleted from the mobile device.
- Photos taken for medical, social care, educational purposes, official purposes shall be stored as part of/within a person's active file, their PCP or within relevant therapists' reports.
- Photos taken for *personal* use of the person we support, shall be given to that person and/or family/guardian/advocate, and then deleted from the Cope mobile device or Cope Foundation's network.
- Photos taken in social, celebratory, or competitive settings, intended for communal areas in Units/Centres, or homes, will generally be considered as 'personal' and belonging to the person/people we support. Once exhibited in communal areas, they should then be offered to the person and deleted from any other storage device on which they are held.
- Centres/Units may identify and retain a small collection of photos for the local archive of the centre. As a guide, 20 photos per occasion may be identified for a local archive to be held on the Cope Foundation computer system in a folder clearly marked as Archive.
- Any photos not filed for medical, social care, educational purposes or officially archived for the centre must be deleted after a period of twelve months.

### 4. Cope Foundation Communication & publicity Use

Explicit consent should be sought for photos/videos taken for Cope Foundation communications purposes; where photos/videos are for sharing through Cope Foundation's website, on Copenet, or for sharing with third party publications or social media channels signed consent must be sought. (Appendix 3)

### 5. Research, Collaboration Projects

Where it is proposed that photos/videos be taken as part of research & collaboration with third parties the advice of the Data Protection Officer should be sought and explicit consent will be required.

## APPENDIX 3 – Photography & Video Recording Consent Form and Guidance



### Cope Foundation Communications & Fundraising Photograph/Video Recording Consent

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Consent to use photos for Communications & Fundraising Uses

No Consent for use of my photo for Communications & Fundraising Uses

Cope Foundation would like to use photos and video/audio recordings of you in different places in order to:

- tell our stories
- create awareness of our services
- raise much needed funds

#### Cope Foundation Communications

Cope Foundation may share my photo(s) on Cope Foundation's own website, on social media, Cope Foundation's intranet (CopeNet) Annual Report, brochures, anniversary publications, Cope Foundation's official archive

'I consent to this use': Tick here

Cope Foundation may share my photo(s) for publication on websites or print publications of other organisations like local newspapers, community groups, and trusted others that Cope Foundation works with or is associated with

'I consent to this use': Tick here

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

(If required) Signature of Advocate (Parent/Guardian/etc.):

- We will always ask before taking photos of you.
- You can let us know if you don't want your photo taken.
- At Cope Foundation events we will always tell you if we have invited newspapers or others to take photos.

**If you change your mind after a photo is taken we will delete photos or stop using them. Contact Jo-Anne Higgins in the Communications and Fundraising Department on 021 464 3346 or email [higginsj@cope-foundation.ie](mailto:higginsj@cope-foundation.ie)**

Photo/Video Consent V2. AU: JH & DPO 01/2019.

Retain: Hardcopy only on Active File. Archive: NO. CR # Pending.



### **Photography/Video Recording: Protocol for Staff**

#### **1. Photos/Video Recordings for Publicity Purposes**

- a) Signed consent (see over) is required where photos/videos are taken for:
- Cope Foundation communications (e.g. CopeNet, Newsletters, posters etc.)
  - Cope Foundation's external publicity (e.g. Cope Foundation's website and social media channels etc.)
  - Sharing with local media and trusted third parties (e.g. community groups, corporate supporters etc.)

#### **2. Photos/Video Recordings for Medical, Social Care, Educational or Celebratory Events**

- a) Signed consent is **not** required where photos/video recordings are taken in order to provide a service (i.e. medical/ therapeutic, social care, education purposes) or taken to celebrate a private event (e.g. a party, in a home, an outing or activity).
- b) When taking a photo(s) for medical, social care, social events, please:
- Be sensitive to the person's preferences
  - Let the person know the purposes of the photo/video recording, who will have access to it, where it will be stored and how long it will be kept.

#### **3. Storage**

- a) Staff should not use their 'personal' mobile device to take photos/videos of people we support.
- b) Photos/videos taken on a Cope Foundation mobile should be sent as soon as possible to the Cope Foundation network for further use or storage and deleted from the mobile.
- c) Photos/videos taken for medical therapeutic, social care purposes will be retained as hardcopy either in a person's Active File/ PCP or in therapists' reports.
- d) Annually or sooner review all photos/video recordings on the Cope Foundation network and delete all unused photos/video recordings.
- e) Annual deletion will be easier if photos are organised.
- f) A long term record of social events, celebrations may be kept. Such collections must be labelled as "Archive" and should be small i.e. no more than 20 photos per event.
- g) Offer individual photos to the person or their family where appropriate.

Photo/Video Consent V2.1 AU: JH & DPO  
01/2019. Retain: Current Copy/Active File.  
Archive: No.



## Appendix 4 – Subject Access Request Form

You/your representative may use this form to request information, and access to information we may hold, about you. Details on where to return the completed form can be found at the end of the form.

### 1. Personal Details: *(Person whose data is being requested)*

Name: \_\_\_\_\_ DOB: \_\_\_\_/\_\_\_\_/\_\_\_\_

Home Telephone No: \_\_\_\_\_ Email: \_\_\_\_\_


Address: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

Are you currently Supported by the Services?

Are you currently Employed by the Service?

Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

 **Go to Section 3.**

### 2. Representatives *(Parent or Next of Kin)*

*Complete only if you are acting on behalf of a person about whom we may hold data*

**Please Note:** *We may still need to contact you or the data subject where proof of authorisation or identity are required*


Representative's Name: [Print] \_\_\_\_\_ Relationship to Data Subject: \_\_\_\_\_

Telephone No: \_\_\_\_\_ Email: \_\_\_\_\_

Representative's Address: *(If different to Section 1 Address of Data Subject)*.

I confirm that I am the authorised representative of the named data subject:

Representative's Name: \_\_\_\_\_ Signature: \_\_\_\_\_

 **Go to Section 3.**

### 3. Specific Details of the Information Requested:

### 3. Completed Forms

**Signed requests to be returned to:**

*Unit/Centre Manager or Central Records Office, Cope Foundation, Bonnington, Montenotte, Cork T23 PT93.*

## Appendix 5 - Access to Records Staff Guidance

It is Cope Foundation's policy that access to copies of the personal records should wherever possible be provided on request under Administrative Access to the person themselves or to their representative.

Confidentiality of personal records is paramount and we are all responsible for safeguarding the privacy rights of people we support and employees.

Verbal requests should be recorded using the Subject Access Request form

The requestor may be asked to verify their identity;

Name and

i) Date of Birth **or** ii) Address.

Central Records Office, Data Protection Officer or Divisional Head shall be consulted prior to release of any records not already in the public domain.

If a Head of Department believes that access should not be provided to certain information contained in a record then, the request must be processed under the Freedom of Information Acts or the Data Protection Acts and the applicant should be notified accordingly.

Where there is uncertainty about offering Administrative Access to records the person should be informed of this and advised of the option of making an application under the Data Protection Acts or Freedom of Information Acts.

The following are examples of records that should not be released routinely:

- Certain information may be of a sensitive nature or infringe on the privacy rights of others.
- Records containing personal information relating to deliberations of an investigation, allegations, complaints and other such information
- Records containing personal information of a deceased person
- Health records where it is considered that access could be prejudicial to the physical or mental well-being or emotional condition of the person
- Where the records involved contain information about a third party
- In circumstances where it is considered that access could be prejudicial to the physical or mental well-being or emotional condition of the person
- In circumstances where it is considered that the record contains matter about a third party received in confidence
- Any other sensitive matter such as documents revealing confidential sources of information.

## Appendix 6 –Data Privacy Notice

 **Cope Foundation**  
Together we can do great things

# Data Protection Notice

Your health and social care records contain important and sensitive information about you and are vital for your care. At Cope Foundation we are committed to:

- keeping your information safe,
- only using it in ways that benefit your care and
- respecting your data protection rights.

### Your Personal Data

- We collect and hold your personal information to provide you with health and social care;
- We collect information directly from you, a family member, a health professional or social worker etc.;
- We will only share your data with people on a need to know basis;
- We will store your data securely and only for as long as it's needed.

### Your Rights

- A right to seek access to your personal information;
- A right to submit a request for us to correct information we hold on you;
- A right to request that we restrict the processing of, delete, or object to the processing of your information in certain circumstances;
- A right to lodge a complaint with the Data Protection Commission (DPC).

**For more information please read our full Privacy Notice at**  
<http://www.cope-foundation.ie/Privacy-Statement>  
**GDPR Enquiries: (021) 464 3360**

## Appendix 7 – Short Privacy Statement

### People we Support & their Families

#### Privacy Statement

You have a right to know about personal data we hold about you and why that information is held.

Cope obtains personal data from you in order to

- provide you with a service
- meet legal and contractual obligations

Cope may also need to obtain relevant information and reports including medical reports that exist within the services listed below

- The Health Service
- Other HSE contracted service providers
- Education Service Providers
- The National Educational Psychological Service
- General Practitioners/Medical Consultants/Other Health Professionals

Cope may need to share personal data with other service providers who are involved in provision of services appropriate to you. This will be done in strictest confidence and on a need to know basis only.

We will store your personal data in accordance with Data Protection Legislation & relevant Cope Foundation policies such as our Data Protection & Records Management policies.

Our full Privacy Statement is available on our website <http://www.cope-foundation.ie/Privacy-Statement>; it includes detailed information about your rights to seek access, rectification and limitation to the processing of your personal data.

*Note: When a person is Under 18, then their family or advocate are to be informed of the person's data protection rights.*

Cope Foundation,  
Bonnington, Montenotte, Cork. T23 PT93.  
Tel: 021 464 3100  
Data Protection Office Tel: 021 464 3360

2018/10 v2 AU; DPO

## Appendix 8

### Rights of Data Subjects General Data Protection Regulation

January 2022

#### What is the GDPR?

The General Data Protection Regulation (GDPR) applies from 25 May 2018.

#### What constitutes personal data?

The GDPR defines 'personal data' as any information relating to an identifiable person, a person we support, their family members, employees, volunteers, students or colleagues (**Data Subjects**) may make a request for a copy of any data we hold relating to them.

#### What are your rights as a Data Subject?

Data Subjects have rights concerning their information. This includes:

- a right to request access to their personal information;
- a right to request us to correct inaccurate information, or update incomplete information;
- a right to request that we restrict the processing of your information in certain circumstances;
- a right to request the deletion of personal information excluding medical records
- a right to receive the electronic personal information you provided to us in a portable electronic format;
- a right to object to us processing your personal information in certain circumstances; and
- a right to lodge a complaint with the data protection commissioner.

#### What is a Subject Access Request (SAR)?

A SAR is a request the data subject can make to request information regarding the data that we hold relating to them and can receive a copy of their personal information. If a Data Subject makes a SAR for their personal information, they are entitled to receive the following information:

- the reasons why their data is being processed;
- the description of the personal data concerning them;
- anyone who has received or will receive their personal data; and
- details of the origin of your data, if it was not collected directly from them.

The information is provided free of charge unless the request is 'manifestly unfounded or excessive'.

#### How to request access my personal data

Data Subjects can access their health records by making a subject access request (SAR) and forms are available for this purpose at <https://www.cope-foundation.ie/Privacy-Statement>

It is also sufficient to write to the Data Protection Office, Cope Foundation. It is important that you provide satisfactory evidence of identification and a sufficient description of the data that you are looking for.

#### Who can request access to personal data

The Data Subject themselves.

The parents or legal guardian where a data subject is under 18

Where a person is over 18 but incapacitated requests may be made by parents or legal guardian based on the data subjects' urgent vital interests or, alternatively, under Freedom of Information.

### **Can a Data Subject ask to delete personal data?**

Data Subjects can submit a request to have personal data deleted however this right is not an absolute right. In most cases we will be legally obliged to keep data for a certain amount of time. We adhere to HSE guidelines for data storage - for full details on how long we store each category of data, please see the [HSE Records Retention Policy](#).

### **How long can personal data be stored for?**

The length of time data can be stored for depends on the type of data. Full details of how long each type of data is stored is in line with HSE guidance - full details can be found in the [HSE Record Retention Policy](#).

### **What can I do if I think my rights haven't been respected?**

If you feel your rights have not been upheld you are entitled to lodge a complaint with the Data Protection Commission (DPC).

**Telephone:** +353 57 8684800  
+353 (0)761 104 800  
**Lo Call Number:** 1890 252 231  
**Fax:** +353 57 868 4757  
**E-mail:** [info@dataprotection.ie](mailto:info@dataprotection.ie)

**Postal Address:**

Data Protection Commission Canal  
House  
Station Road  
Portarlinton  
R32 AP23 Co. Laois

### **Contacting the Cope Foundation Data Protection Office?**

Please contact our Data Protection Office:

- If you have any queries in relation to Data Protection or other issues around the security of your personal information
- For more information about the steps we are taking to protect your information
- For more information about your rights, including the circumstances in which you can exercise them and how to exercise them,
- If you wish to raise a complaint on how we have handled your personal information, you can contact our Data Protection Officer who will investigate the matter. We hope that we can address any concerns you may have.

**Data Protection Office: (021) 464 3360**

**Email: [oflynns@cope-foundation.ie](mailto:oflynns@cope-foundation.ie)**

### **Useful Links:**

HSE GDPR Website: <https://www.hse.ie/eng/gdpr/>

Data Protection Act:

<http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print.html> DPC GDPR

Website: <http://gdprandyou.ie/>

GDPR: <https://gdpr-info.eu/>