Data Protection Policy & Guidelines

Document Control	
Authorised by:	Colette Kelleher, Chief Executive
Date:	May 2014
Review Date:	May 2017
Document Review History	
Previous Document:	Data Protection Policy & Guidelines 2009
Amended (Y/N):	Yes

CONTENTS

PART 1: Policy

1.1 The Eight Data Protection Principles

Under the Data Protection Acts, 1988 and 2003, COPE Foundation as a Data Controller has a legal responsibility to:

1. Obtain and process information (Data) fairly;
2. Keep Personal Data only for one or more specified, explicit and lawful purposes;
3. Process Personal Data only in ways compatible with the purposes for which it was given initially;
4. Keep Personal Data safe and secure;
5. Keep Personal Data accurate, complete and up-to-date;
6. Ensure that Personal Data is adequate, relevant and not excessive;
7. Retain Personal Data no longer than is necessary for the specified purpose or purposes;
8. Provide a copy of his/her Personal Data to any individual, on request.

1.2 Policy Statement

COPE Foundation as a Data Controllerôwill endeavour:

- To comply with both the Data Protection Acts 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 Foundationôs possession is kept safe and secure;
- To support staff to meet their legal responsibilities particularly as set out in the Eight Data Protection Principles;
- To respect individualsôrights;
- 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 handle Personal Data of the people we support and/or staff.

1.5 Definitions/ Descriptions

'Access Request' is where a person makes a request to an organisation for the disclosure of their Personal Data, under section 4 of the Data Protection Acts.

'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.

'Sensitive Personal Data' relates to specific categories of Data which are defined as Data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions, or the alleged commission of an offence; trade union membership.

The Data Protection Acts 1988 & 2003 (the 'Data Protection Acts') 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

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 Eight Data Protection Principles, in order to safeguard the privacy rights of individuals.

2.2 Obtain and process information (data) fairly

To fairly obtain information, the Data Subject must, at the time their Personal Data is collected, be made aware of the following:

- The name of the Data Controller: COPE Foundation;
- The purpose in collecting the Data;
- The persons or categories of persons to whom the Data may be disclosed;
- The existence of the right of access to their Personal Data;
- The right to rectify the Data if inaccurate or processed unfairly;
- Any other information which is necessary so that processing may be fair and the Data Subject has all the information necessary in relation to the processing of their Data.

To ***fairly process Personal Data****,* it must have been fairly obtained, and the Data Subject must have given consent to the processing,

Or

The processing must be necessary for one of the following reasons:

- The performance of a contract to which the Data Subject is a party;
- In order to take steps at the request of the Data Subject, prior to entering into a contract;
- Compliance with a legal obligation, other than that imposed by contract;
- To prevent injury or other damage to the health of the Data Subject;
- To prevent serious loss or damage to the property of the Data Subject;
- To protect the vital interests of the Data Subject, where it is inappropriate to get their consent;
- Where seeking the consent of the Data Subject is likely to result in their interests being damaged;
- For the administration of justice;
- For the purpose of the legitimate interests of COPE Foundation, except where the processing is unwarranted in any particular case, by reason of prejudice to the fundamental rights and freedoms and legitimate interests of the Data Subject.

To ***fairly process Sensitive Personal Data***, it must be fairly obtained and the Data Subject must give explicit consent (or where they are unable to do so for reasons of incapacity or age, explicit consent must be given by a parent or legal guardian) to the processing,

Or

The processing is necessary for one of the following reasons:

- For the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the Data Controller in connection with employment;
- To prevent injury or other damage to the health of the Data Subject or another person;
- To prevent serious loss or damage to property;
- To protect the vital interests of the Data Subject or of another person in a case where, consent cannot be given, or the Data Controller cannot reasonably be expected to obtain consent;
- For the purpose of obtaining legal advise, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights;
- For medical purposes (appendix 1);
- For the purpose of the assessment or payment of a tax liability;
- In relation to the administration of a Social Welfare scheme;
- It is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation;
- The information being processed has been made public as a result of steps deliberately taken by the Data Subject.

2.3 Only keep personal Data for one or more specified, explicit and lawful purpose(s)

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.

2.4 Process Personal Data only in ways compatible with the purpose for which it was given initially

- 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 the 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 fulfill official employment duties.

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;
- Where it is required by law;
- Where it is required for legal advice or legal proceedings, and the person making the disclosure is a party or a witness;
- 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, or serious loss of or damage to property.

2.5 Keep Personal Data Safe and Secure

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 Foundationôs 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 USBôs are used;
- Personal Data is not to be stored on portable devices except in essential circumstances. Where deemed essential, the Data 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 Foundationôs security measures, and comply with them;
- All waste papers, printouts etcetera to be disposed of appropriately.

2.6 Keep Personal Data accurate, complete and 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 Ensure that Personal Data is adequate, relevant and not excessive

- Only information necessary for the stated purpose should be collected, nothing more.
- A periodic review should be carried out by managers and their staff team, to 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.
- Periodic reviews should take place of any Personal Data already held, to make sure it is adequate, relevant and not excessive for the purpose for which it was collected.

2.8 Retain Personal Data 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;
- COPE Foundations Records Management Policy 2014 which includes time factors for the retention and destruction of data in manual and electronic form is to be adhered to;
- Personal Data should be disposed of securely when no longer required. The 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 PCs or laptops are transferred from one person to another, or when being disposed of.

2.9 Provide a copy of his/her Personal Data to any individual, on request

On making a written request under Section 4 of 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 40 days to:

- A copy of the Data being kept about him/her;
- 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;
- Know the reasons involved in decisions made about the Data Subject;
- 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.

To make an access request the Data Subject must:

- Apply in writing (which may be via email);
- Give any details which might be needed to help identify him/her and locate the information kept about him/her.

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.

2.10 Consent to Photographs/Video/Audio Recordings (Appendix 2)

- 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.
- In all instances (*save where the photograph, video and/or audio recording is taken for medical purposes as contemplated in appendix 1*) where a photograph is taken, a video or audio recording is made, the **explicit consent** of the person and/or their parent/guardian/advocate should be sought for its use or publication in any medium, for example in the local newspaper, annual report or a website.
- 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.

PART 3: Compliance Audits (Risk Management)

3.1 Internal Compliance Audit

- The principle purpose of an Internal Compliance 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 will be undertaken by members of the Data Protection Working Group (DPWG: appendix 3) in order to identify existing and potential risks;
- Internal Compliance Audits will review both manual and electronic data procedures and compliance;
- Whilst Internal Compliance Audits will be primarily questioned based and addressed to the Head of Division and/or the Manager of the Unit/Centre, site visits will take place, and a random sample of records will be examined to ensure that good practice is in evidence;
- The majority of the questions in the questionnaire will be typically structured around the Eight Data Protection Principles, and *COPE Foundation's Records Management Policy;*
- Immediate remedial action may be prescribed by the DPWG in order to ensure that the requirements of the Data Protection Acts are observed;
- It will be a requirement that Managers/ Staff cooperate fully with members of the DPWG in completing Internal Compliance Audits questionnaires and site visits;
- The results will be recorded.

3.2 External Compliance Audit

- External Compliance Audits of all aspects of Data protection within COPE Foundation may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

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;
- Equipment failure;
- Human error e.g. misaddressing an email 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. ósocial engineeringô 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 without delay by staff to their Line Manager, who in turn will immediately notify the Head of Quality, Systems and Shared Services and/or the FOI/Data Protection Officer with the Incident Details.
- The Data Breach Management Team (DBMT: appendix 3) (and if considered appropriate by the DBMT, any other individual) will immediately convene to deal with the data breach incident.

- The team will 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 individualsô 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 Foundationôs 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).

- The FOI/Data Protection Officer will be responsible for contacting the ODPC at 1890-252-231 or info@dataprotection.ie to inform them of the Data breach.

- The Data Breach Management Team (DBMT), in consultation with the Office of the Data Protection Commissioner (ODPC), will decide in the particular circumstance, if it is appropriate to inform the persons whose Data has been breached. In this regard, COPE Foundation will be aware of the dangers of óover notifyingô, as not every incident will warrant notification.

- When notifying individuals, the DBMT 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 ongoing 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.

- Other statutory agencies, such as the Health Service Executive may also need to be informed.

4.2.3 **Evaluation & Response**

Subsequent to any data/information security breach, a thorough review of the incident will be made by the DBMT. 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 employeeôs professional career in COPE Foundation.

5.3 Data Protection Support

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

CONCLUSION

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.

APPENDICES

APPENDIX 1

Processing the Data of People we Support for Medical Purposes

1.1 Data/Information

Includes photographs, video/ audio recordings for ómedical purposesô(see 1.5 below).

1.2 Consent Required?

Consent is <u>not</u> required where the processing of Data/ information is necessary for ómedical purposesô, and is undertaken by:

- A Health Professional, <u>or</u>
- 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.

1.3 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 ï Data Protection (Access Modification) (Health) Regulations, 1989).

1.4 Medical Purposes

- The definition of ôMedical Purposesôincludes the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment, and the management of healthcare services.

1.5 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 Acts 1988/2003 s.2B(1)(b)(viii) & s.2B(4)]

APPENDIX 2

Consent to take Photographs or Make Video/ Audio Recordings of People we Support

2.1 Recommended Good Practice

- This Good Practice Guidance is aimed at those who work in Units, Centres & Schools of COPE Foundation;
- Where the Data Protection Acts do apply, a common sense approach suggests, that if the person taking the photograph or the video/ audio recording, asks for permission to do so, and it is granted, this will usually be enough to ensure compliance;
- Photographs, video/ audio recordings taken of people we support for official use (see 2.2.2 below), may be covered by the Acts, and those people and or their families/ guardians should be advised, and their consent should be sought;
- Photographs, video/ audio recordings taken purely for personal use are exempt from the Data Protection Acts.

2.2 Examples

2.2.1 Personal Use

- A parent takes a photograph of their child and some friends taking part in the school sports day, to be put in the family photograph album. These images are for personal use and the Data Protection Acts do not apply.
- Grandparents are invited to the Unit for an in-house birthday party or Christmas concert and they wish to make a video/ audio recording of it. These images are for personal use and the Data Protection Acts do not apply.

2.2.2 Official COPE Foundation Use

- Photographs of people we support are taken for identification purposes. These images are likely to be stored electronically with other personal data, and the terms of the Data Protection Acts will apply. Written consent should be sought.
- A small group of pupils/people we support are photographed during a lesson or activity, and the photo is to be used in the school prospectus or annual report. This will be personal data, but used in a public way. Written consent should be sought.

2.2.3 Media Use

- A photographer from a local newspaper takes photographs of 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.

2.2.4 Photographs of People we Support taken by COPE Foundation Staff

- Photographs or video/ audio recordings must be either for:

  1. Personal Use, *or*
  2. Official Use (other than for ómedical purposesôas contemplated in Appendix 1).

- The following question must be answered before photographs or video/ audio recordings are made of people we support: Are the photographs and/or video/ audio recordings intended for the personal use of the person we support, or for the official use of COPE Foundation?

- Where photographs are for the *personal* use of the person we support, they must be given to that person and/or family/guardian/advocate, and then deleted from the camera memory, or any COPE Foundation computer filing system.

- Where photographs are taken of people we support in social, celebratory, or competitive settings, and are intended for communal areas in Units/Centres, or Schools, these photographs will generally be considered as ópersonalôand belonging to the person/people we support. Once exhibited in communal areas, they should then be deleted from the camera memory and/or any other storage device on which they are held.

- Where photographs are for COPE Foundation archives, they may be held on a COPE Foundation computer system for a maximum period of twelve months, after which they should be downloaded to the appropriate medium, and deleted from the computer system.

Appendix 3

Data Protection Working Group

- Marguerite OõBrien, Head of Quality, Systems & Shared Services
- Mary Fleming, Manager of Central Records Office
- Bernie OõSullivan, Head of Homes & Community 2 Division
- Chris Traynor, FOI/Data Protection Officer