Data Protection Procedure

This procedure implements the Information Governance Policy providing information on Data Protection and outlining the processes needed to ensure compliance with all legislative, regulatory and best practice requirements. It seeks to ensure the ethical, secure and confidential processing of information and use of information systems to support the provision of high quality care.

BACKGROUND

In drafting this Procedure, the following legal and regulatory obligations and best practice guidance have been considered:

- General Data Protection Regulation (GDPR);
- Data Protection Act 2018 (DPA 2018);
- Mental Capacity Act 2005;
- Common Law standards;
- The Care Standards Act 2000;
- The Human Rights Act 1998;

Definitions taken from GDPR

Personal data is:-

> 'Any information relating to an identified or identifiable natural person ('data subject')'

Processing is:-

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

Processing subject to the GDPR is:-

> 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'

Filing system within the GDPR is:-

‘any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis’

Special Categories of Personal data is personal data revealing:-

- ‘Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health;
- Data concerning a natural person’s sex life or sexual orientation’.

Data Protection & other Guides

Further detail on the issues contained in this Procedure can be found in the relevant Data Protection Guides available to all staff on SharePoint.

As there is some overlap between many of the information-related procedures, additional information may also be found in the Confidentiality, Information Governance and Information Risk Management procedures and guides available to all staff on SharePoint.

Any queries should be referred to the Data Protection Officer.

PROCEDURE format

A. Roles and responsibilities
B. The Data Protection Principles
C. Lawful basis for processing
D. Consent to process data
E. Accountability
F. Individual rights
G. Notification and reporting

A. Roles and responsibilities

Data Protection Officer

Young Epilepsy has determined that, under the GDPR/DPA 2018, it is legally obliged to appoint a Data Protection Officer (DPO). The DPO informs and advises the organisation on data protection obligations, monitors compliance with data protection laws and is the first point of contact for supervisory authorities and for individuals.

The DPO may be contacted on dpo@youngepilepsy.org.uk and on ext. 286.

Senior Information Risk Owner (SIRO)

The SIRO is a member of the Exec team, who is responsible for overseeing Information Governance (IG) risk, including those related to Data Protection, and implementing the organisation's information risk strategy.

The Information Governance Steering Group (IGSG)

The IGSG is responsible for driving the overall promotion and implementation of Data Protection throughout Young Epilepsy. It must annually review and approve all Data Protection related procedures.

All staff

All employees are responsible for adhering to the GDPR/DPA 2018 and Young Epilepsy's own Data Protection policies, procedures and guides. Failure to do so may be considered gross misconduct and can result in disciplinary action.

B. The Data Protection Principles

All processing undertaken by Young Epilepsy staff must meet the Seven Principles of the Data Protection Act.

Personal Data must be:-

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data.

The Data Controller must:-

7. Responsible for, and be able to demonstrate compliance with the GDPR.

C. Lawful basis for processing

Young Epilepsy staff may only process personal data or special categories of personal data if there is a legal basis for doing so. This must be identified, recorded and implemented prior to undertaking the processing.

For personal data, the following provide a lawful basis:

a. Undertaken with the consent of the data subject; or

b. Necessary for the performance of a contract with the data subject or to take steps to enter into a contract; or

c. Necessary for compliance with a legal obligation; or

d. Necessary to protect the vital interests of a data subject or another person; or

e. Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

f. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (When relying on this lawful basis, the Legitimate Interests Assessment form must be completed.)

For special categories of personal data, the following provide a lawful basis:

a. Undertaken with the explicit consent of the data subject; or

b. Necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement; or

c. Necessary to protect the vital interests of a data subject or another person; or

d. Carried out in the course of legitimate activities of a not-for-profit body; or

e. Relates to personal data manifestly made public by the data subject; or

f. Necessary for legal purposes; or

g. Necessary for reasons of substantial public interest in UK or EU law; or

h. Necessary for medical purposes; or

i. Necessary for reasons of substantial public interest in public health; or

j. Necessary for public interest archiving purposes, scientific or historical research purposes or statistical purposes.

There must be no breach of:

- Confidentiality *(Please refer to the Confidentiality Procedure and Guides);*
- The ultra vires rule and the rule relating to the excess of delegated powers, under which the data controller may only act within the limits of its legal powers;
- Legitimate expectation, that is, the expectation of the individual as to how the data controller will use the information relating to him;
- Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence).

D. Consent to process personal data

Where possible consent to process personal data and/or explicit consent to process special categories of personal data should be obtained.

Consent

In line with Young Epilepsy's consent procedure, it should be sought as follows:

a. From the individual concerned:
    - Where that individual is over 16 years of age and has capacity under the Mental Capacity Act;
    - Where that individual is under 16 years of age, but, as applicable, has Gillick competency/ meets the Fraser Guidelines.

b. From parents, where the individual is under 16 years of age and lacks Gillick/ Fraser competency;

c. From a supporting best interests decision, where the individual is over 16 years of age and does not have capacity under the Mental Capacity Act 2005;

d. From a Deputy or Attorney, where one has been appointed to make a decision in the area concerned.

Mechanisms of consent

Consent to process data is obtained through one of the following three mechanisms:-

a. Privacy Notice relevant to the individual (such as the staff, student and fundraising privacy notices):

b. Existing consent forms, (such as the Standard Student Consent forms and the Staff Employment Contract and Handbook);

c. Ad hoc or issue specific consent forms, which are drafted upon request by the DPO.

Staff are expected to regularly review student consents to ensure that they continue to be appropriate and accurately reflect the student/parents' current views.

The Human Resources department is responsible for retaining a record of all staff consent.

Consent must be obtained whenever information is to be processed or disclosed in a manner that is not consistent within any existing consents or other lawful basis. The employee who intends to undertake the processing/ disclosure of information is responsible for ensuring consent is in place in such circumstances.

E. Accountability

Young Epilepsy seeks to ensure accountability by using the following mechanisms:-

- Appointment of a Data Protection Officer;
- Certifications and codes (where relevant);
- Contractual requirements and standards that staff must ensure are included in all contracts where the processing of personal data is to be undertaken;

- Data Protection by Design and default, which means that all staff must consider Data Protection at the start of all initiatives that involve personal data;
- Data Protection Impact Assessment, which forms part of the IG Compliance process (please refer to the IG procedure and related guides);
- Documentation of processing, including the use of the Summary of Processing forms or other record formats.

F. Individual Rights

Young Epilepsy staff must process data within the data subject's rights as specified in the GDPR/DPA 2018. These are:-

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

N.B. Young Epilepsy does not currently undertake any processing that relates to portability or any automated decision-making and profiling.

Internal process

All requests to exercise any of the above rights must be immediately forwarded to the DPO for management within the terms of the GDPR/DPA 2018.

G. Notifications & reporting responsibility

Data Protection Registration with the ICO

The DPO is responsible for the annual registration of the following with the ICO:

- NCYPE/Young Epilepsy
- NCYPE Pension Scheme

The Executive are responsible for informing the DPO of any substantial changes to Young Epilepsy processing, which will require the Registration to be amended.

IG incident reporting

Where a breach is likely to result in a risk to the rights and freedoms of individuals the ICO must be informed within 72 hours and the Reporting Tool on the Data Security & Protection Toolkit should be used for this.

This procedure is agreed by the Director of Business Development and will be implemented by all departments.

Signed: ..... **Date: .....**

Tim Moore, Director of Business Development & Senior Information Risk Owner

Date of next review: 31 March 2020