Data Protection Policy (including GDPR)

Approved by: Board of Trustees

Policy owner: Director of Finance

Issue date: June 2018

Review date: June 2021

Data Protection Policy

Beat are committed to responsible use of data in relation to all our stakeholders information and compliance with the General Data Protection Regulations (GDPR) and The Privacy and Electronic Communications Regulations (PECR).

GDPR applies to all 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified from that data. GDPR applies to automated personal data and manual filing systems.

PECR gives people specific privacy rights in relation to electronic communications.

Under the GDPR, the data protection principles set out the main responsibilities we must follow at beat. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- 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
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

To ensure we can comply with the principles we are committed to protecting individual rights. Please see appendix 1 for full details about subject access rights.

If any data breaches do occur we have a clear policy and process for reporting (link to data breaches). All staff receive information and training about reporting data breaches.

To ensure data protection is carried out diligently across the organisation Beat has committed to:

- Having a named data controller supported by a GDPR working group (see appendix 3 for details)
- Appointed data champions across the organisation
- Data Protection training provided to all staff and volunteers and refreshed every 2 years.
- Maintain a register of all data processors we are working with detailing their commitment to comply with GDPR regulations
- When dealing with new types of data we will carry out a data protection impact assessment. These will be reviewed as necessary to they are accurate and sufficient
- We have a clear procedure for reporting data breaches (see appendix 2)

All data held by Beat is identified as to its sources, where it is held, who has access, the lawful basis for holding and processing data and the period of time is should be held for.

In addition special category data (usually relating to health information) is treated very carefully and a condition for processing is identified in addition to the lawful basis.

A full data audit was carried out in 2018, this will be reviewed and updated with executive scrutiny and summary reporting at board level at least annually.

We have clear, tailored privacy statements, which are communicated to all stakeholders and are available on our website.

Where the basis for holding information is consent, this consent is obtained clearly to ensure the data subject fully understands what data beat will be holding and how it will be used.

This policy should be read in conjunction with other policies that relate to processing and retaining information: Confidentiality Policy (add link)

Protecting Children and Vulnerable People Policy (add link)

For further information, detail and guidance please refer to the Information Commissioners Office (ICO) https://ico.org.uk

Appendix 1

Subjects Access Rights (SARs)

All individuals for whom we hold or process data has the following rights. Any requests received to exercise these rights should be shared with the GDPR working group who will co-ordinate the response within the required timeframe.

For further detail on the rights below please refer to the Information Commissioners Office (ICO) https://ico.org.uk

Right to be informed

Data subjects can contact Beat as the data controller and request information on what data is held and processed

Right of access

Access to personal data may be requested to verify and ensure data processing is lawful

Data must be provided to the data subject within one month of the request or two months by extension if the request is complex. Data must be provided free of charge unless the requests are unfounded or repetitive. The identity of the subject must be confirmed before any response is made

Data can be provided in paper form or secure electronic means (e.g. encrypted email)

Right to rectification

If data held is inaccurate or incomplete a data subject can ask for it to be rectified. This must be done and a response sent within one month of the request (or two months by extension if the request is complex). If we do not feel data can or should be rectified we need to inform the data subject of this and provide details about their right to complain to ICO

Right to erasure (right to be forgotten)

A data subject has the right to request that their data is permanently deleted. There is only an obligation to destroy data if it was obtained as a result of consent which has now been withdrawn or the data is no longer needed for the original purpose for which it was obtained.

If there is a legal reason to keep the data the right of erasure can be refused.

Erasure does not need to apply to all data, data that is unreasonably difficult to access such as that kept in a remote archive will not necessarily need to be erased.

The data subject must be informed when the data is erased or the reason their right to erasure has been refused.

If data has been shared with third parties they must be informed of the erasure request.

Right to restrict processing

In the interim period where a right to erasure is being considered the data processor or controller will only be able to store limited data and will not be able to process it.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows an individual to move, copy or transfer data easily from one IT environment to another in a safe and secure way without hindrance to usability. This only applies where consent was given to collect and process data initially and the process is done by an automated means.

Requests must be completed within a month and we must respond to the individual is we are not able to comply making them aware of their right to complain.

Right to object

Data subjects have the right to object if they feel their data is being processed or stored inappropriately. The right is absolute and all data processing must be stopped if data is used for marketing purposes. Where other basis are used to obtain, hold and process information the subject must demonstrate ground relating to his or her particular situation

Rights re automated decision making and profiling

Automated decision making and profiling is allowed only when it is necessary and must be based on an individuals explicit consent. It is prohibited if it can adversely affect someone’s legal rights.

Appendix 2

Personal Data Breaches

To comply will GDPR and to safeguard personal information Beat will report personal data breaches without delay (within 72 hours of the breach being identified). The purpose of data breach reporting is to mitigate potential losses to the organisation and any individuals affected and to improve systems and training.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

All data breaches must be logged on a data breach form and sent to admin@beateatingdisorders.org.uk with the subject line Confidential Data Breach. The information will be forwarded to a member of the GDPR working group. All breaches will be examined to identify further actions which could include:

- Reporting to Information Commissioners Office (if the breach is likely to risk an individuals rights and freedoms)
- Make the individuals who data has been breached aware
- Providing further training and guidance to prevent re-occurence

Appendix 3

Data Protection Roles

Data Protection Manager: Rebecca Field- Head of Communications
r.field@beateatingdisorders.org.uk 01603 753310

GDPR Working Group: Claire Reynolds- Director of Finance and Resources
c.reynolds@beateatingdisorders.org.uk 01603 753306

Diane Rhodes- Supporter Development Manager
d.rhodes@beateatingdisorders.org.uk 01603 753325

Sue Sparks- Office Manager

s.sparks@beateatingdisorders.org.uk 01603 753305

Rebecca Field- Head of Communications
r.field@beateatingdisorders.org.uk 01603 753310

Data Champions: London: TBC- Contract delivery and Outcomes lead

Warrington: Katie Gledhill-Taylor-Senior helpline advisor