Confidentiality Policy

Approved by: Board of Trustees

Policy owner: Director of Services

Issue date: June 2020

Review date: June 2021

This confidentiality policy sets out the Charity's practices and procedures on the disclosure of personal information relating to service users.

The great majority of occasions when this policy will apply relate to the interactions between service users and Beat's telephone and online services. Staff and volunteers working in other areas may encounter situations where this policy should be applied and, in such cases, should interpret the policy to the specific circumstances. Reference to the safeguarding and data protection policies, and the Designated Safeguarding Officer, would also be expected.

1. **Purpose for this Policy Statement**

- To protect the interests of our service users.
- To ensure all service users have trust and confidence in the Charity and that their dignity is respected.
- To protect the Charity, its trustees, staff and volunteers.
- To comply with data protection law.

2. **Who this policy applies to:**

This policy applies to all employees, freelancers, interns, contractors, trustees and volunteers of Beat and to those who are visitors to the organisation.

3. **Obligations/requirements**

All personal information about service users, their carers and families will be treated as confidential.

Information will only be collected that is necessary and relevant to the work in hand. It will be stored securely, only accessible on a need to know basis to those members of staff and volunteers duly authorised.

The personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

Our confidentiality policy is explained at the start of every contact and service users are asked to confirm they understand.

Service users requesting ongoing support will be asked to give their verbal consent. This will authorise Beat to keep written computerised records of the service user's personal details and the support provided.

Where consent is not given for Beat to record and store basic information about the service user an anonymised record will be made.

Confidentiality will never be broken without informing the caller and identifying information will never be sought without clear explanation of why the data is being collected.

4. **When we will break confidentiality**

Beat will break confidentiality and share information with other agencies only under the following circumstances:

- To ensure the safety and welfare of the service user
- Where such information is required to ensure the safety and welfare of the persons concerned in the care of the service user

- To protect the safety and welfare of, and prevent serious harm to, a child or other adult who may be at risk.
- A service user gives them certain information relating to terrorism

5. Breaching confidentiality

If a contact presents as at risk of significant harm, they will be encouraged to seek support by contacting emergency services or another appropriate agency (NSPCC, local crisis team, ChildLine, Samaritans).

If the contact is not ready, able or willing to contact the appropriate organisation and identifying information about the caller is known, the Helpline Supervisor on shift will contact the Designated Safeguarding Officer to discuss the safeguarding concern and whether breaking confidentiality is necessary to share information with relevant agencies and emergency services.

If a decision is made to breach confidentiality and another agency/emergency service is to be contacted, the advisor will inform the service user at the earliest opportunity with a clear explanation.

When a decision is taken to break confidentiality, then all available identifying information should be released to the appropriate authority. This includes telephone numbers (if immediately available), email addresses and IP addresses if given by the service user and not automatically gathered at the point of contact by computing systems. Information gathered by computing systems will only be released if requested by the police.