SP-UK

SUICIDE PREVENTION UK

Suicide Prevention UK

Confidentiality Policy

2024

Introduction and Purpose

As a Charity dedicated to providing support and assistance to individuals facing mental health challenges, we understand the critical importance of confidentiality in fostering a safe and trusting environment.

This policy has been written to protect the Charity and its stakeholders from breaches of confidentiality by clarifying what confidential information is and defining controls around how our staff members should act when they are aware of confidential information.

Scope

This policy applies to all who work for or on behalf of Suicide Prevention UK and have access to personal, sensitive and confidential information.

Definitions

Confidential information refers to any data or information, whether written, oral, electronic, or otherwise, that is not publicly available and is considered private or sensitive. This can include personal details (such as names, addresses, and contact information), medical records, criminal records, unpublished financial information, legal documents, business strategies, and any other information that is disclosed in a relationship of trust and with the expectation that it will be kept secret.

Authorised individuals are those people with a legitimate need to process that information. Typically, authorisation is role-based, meaning only certain roles within an organisation are permitted to process, access, share, etc., specific types of confidential, personal or sensitive data.

Information can be **shared** when there is a lawful basis to do so, and the sharing complies with the principles of data protection, including obtaining explicit consent when required and ensuring data minimisation, security, and accountability.

Please also see our GDPR Policy, Whistleblowing Policy and Safeguarding Policy for further information on when and why confidential, personal and sensitive information can be shared and with whom it may be shared.

Policy

General Principles

- Access to highly confidential and/or sensitive information is restricted, and staff members will only be given access to such information on a need-to-know basis.
- Staff members must consider all information they have access to or are given because of their work or volunteering as confidential unless advised otherwise.
- Staff members must ensure the security of any confidential, personal or sensitive information that comes into their possession.
- When sharing personal and sensitive information with others, there are specific laws governing when confidentiality may be broken. Therefore, staff members shall not at any time, whether before or after their employment, service contract or volunteer tenure, disclose confidential information to any person outside of the organisation or through any other communication method without the Board's prior written consent unless there is a legitimate need to override this (see the 'Disclosure' section below and Appendix A).
- Confidential, personal and sensitive information, where there is a legal basis to share it, must be shared using secure methods of communication.

Discussions and Meetings

- If discussing an identifiable person in a meeting, staff members should only disclose personal or sensitive information relevant to the matter at hand.
- Staff should be aware that others may be able to overhear. Therefore, sensitive discussions should only happen in an appropriately private place.
- Meeting minutes that contain personal or sensitive information must be marked as private and confidential and only accessible to those with a need-to-know.
- The same principles apply to confidential Charity information.

Outside of Work

- Staff members must not gossip about confidential Charity information, their colleagues, or those we aim to help. This includes revealing personal and sensitive information about an identifiable individual.
- When working remotely, all confidential, personal and sensitive information should be kept secure.

Breaches of Policy

If any staff member becomes aware of a breach of confidentiality, they should inform the trustees immediately.

All breaches will be thoroughly investigated, and any breach of this policy may lead to sanctions under the Disciplinary Policy.

Monitoring and Reviewing

This policy should be reviewed periodically to ensure that it remains compliant with current legislation, meets best practices, and is not discriminatory.

Suicide Prevention UK will monitor the number of complaints and the type of complaints received.

The results of monitoring will be reviewed by the senior management at regular meetings.

Where evidence or trends indicate that our culture, policy, procedures, or workforce require intervention, an action plan will be initiated.

Policy Date: November 2020

Review Date: April 2024

Next Review: April 2025

Dated and Signed by the Chair and Founder of Suicide Prevention UK:

Appendix A: The Law - Sharing Information and Breaking Confidentiality

In the UK, there are specific circumstances under which it is lawful and, at times, necessary to break confidentiality and share personal and sensitive data. These exceptions are governed by legal and ethical frameworks designed to protect individual and public interests. Our policy acknowledges these circumstances, ensuring that any breach of confidentiality is justifiable, proportionate, and in compliance with the following conditions:

1. **Legal Obligation**: When required by law, such as under court orders, statutory requirements, or specific legal provisions, we must disclose the necessary information. For example, the reporting of certain infectious diseases, safeguarding concerns, or financial transactions that are subject to legal scrutiny.
2. **Consent**: If the individual or their legal representative has given explicit consent to share their information, we may lawfully disclose it in accordance with their wishes and the parameters of the consent provided. For example, a new starter may give consent to share that they have a disability with other staff whom they may encounter.
3. **Public Interest**: In situations where non-disclosure could result in harm to others or to the public, it may be necessary to breach confidentiality. For example, cases where there is a risk of serious harm, abuse, or threats to public health and safety.
4. **Vital Interests**: When there is an immediate and critical risk to the life or physical safety of the individual or others, and the individual is incapable of giving consent (due to incapacity or emergency circumstances), it is permissible to share relevant information to prevent serious harm or death. For example, if an individual is threatening suicide, information about them may be shared with Police and paramedics without consent.
5. **Regulatory and Inspection Requirements**: When regulatory bodies or inspectors have a legitimate and lawful request for access to confidential information as part of their duty to enforce standards and regulations, we must comply with such requests, ensuring that the scope and purpose of the information shared are clearly defined and legally justified.

In all cases of breaking confidentiality, the decision must be approved by the Founder and CEO and documented, including the rationale for disclosure, the details of the information shared, and the parties with whom the information was shared. This documentation is essential for accountability and for reviewing the appropriateness of the actions taken.