BATTLE SCARS CIO CONFIDENTIALITY POLICY

Policy information	
Organisation	Battle Scars
Scope of policy	Applies to all services, activities, training and general running of the organisation.
Policy operational date (original)	06/02/18
Policy prepared by	Jenny Groves – CEO
Date approved by Board	15/01/24
Reviewed on **Reviewed by**	06/01/24 Jenny Groves - CEO
Amended	No
Policy review date	By 31/01/26 Every 2 years
Distributing	This policy will be available on the Battle Scars website. It will be a requirement for all trustees and staff to read the policy after appointment or after its review. A summary of all relevant policies will be included in the volunteer handbook with clear signposting to the full text. Volunteers will be kept up to date with any changes that might affect their role.
Confidentiality	
Definition	For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of the organisation through its work.
Confidentiality & Data Protection	Confidentiality and Data Protection DO NOT cover the same things. Some things are confidential but are not subject to Data Protection: • Identifiable experiences, explanations and opinions expressed by service users. • Information which is not recorded either on paper or electronically. • Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act.
Basic parameters	• The organisation holds personal data about its staff, service users, volunteers, members etc which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission. • All personal data will be dealt with sensitively and in the strictest confidence internally and externally. • Access to information is on a 'need to know' basis. No one will have access to information unless it is relevant to their work.

	• In work with young people under the age of 18 we will keep anything disclosed as confidential and will only share with their parents / carers what the young people are happy for us to share unless keeping such information confidential puts the young person or another person in danger. • Confidentiality will be broken if a disclosure is made regarding a serious immediate risk to a service user's life or health or relating to their wellbeing (in case of abuse). Action will be taken according to our Protecting Vulnerable Adults and Safeguarding Children policies. Any such action will be fully explained to them unless they are in no position to understand (e.g. unconscious or very young).
Communication with service users	• The confidentiality rule in the group agreement for support groups is explained to all new service users. • Service users will be made aware of the existence of this policy which can be easily accessed via our website.
Communication with volunteers & staff	All volunteers and staff will receive training on how to treat disclosed information with clear procedures, ongoing support and supervision.
Communication with members	All personal data on membership forms will remain confidential.
Security	
Setting security levels	Volunteers and staff will receive training if linked to their work to avoid breach of confidentiality to be made especially aware of cases where breach of confidentiality could have great consequences (e.g. when dealing with abuse of young people under the age of 18)
Security measures	• All personal paper-based and electronic data will only be accessible to those individuals authorised to have access. • No data to be left where it can be read by others who are not volunteers, employees or trustees directly involved. • IT equipment is password, PIN or fingerprint protected restricting access to databases to authorised volunteers and employees only. • IT equipment is protected by antivirus and anti-hacking software. • Secure cloud storage is used.
Specific risks	If a volunteer or employee is put under pressure to disclose confidential service user information by a parent, support worker, mental health professional etc. it should be reported to the CEO or one of the trustees within 24 hours using emergency contact details (either the Battle Scars mobile phone or the CEO's)
Storage	*See Data Protection Policy*
Volunteer & employee access to own files	All volunteers and employees have the right to view their files.
Disclosure & transmitting	
Disclosing information	If a report is being written or a service user is asking the organisation to liaise with, disclose information to or share information with any third party, statutory or voluntary agency the organisation will:

	• discuss the possible implication of any disclosures with the person or persons concerned before they are made; • ascertain who will have access to the information. Battle Scars will remind all service users and especially those meeting in a group setting about the needs for confidentiality. However, the organisation cannot guarantee that service users will comply with this request.
Transmitting confidential information	Battle Scars will have a secure system for the transmission of confidential information by email. The email should include the following information: • "This email is strictly confidential and is intended for use by the addressee. If you are not the intended recipient, any disclosure, copying, distribution or other action taken in reliance of the information contained in this email is strictly prohibited." • "If you receive this transmission in error, please use the Reply function to tell us and then permanently delete what you have received." Confidential letters will be clearly marked "private and confidential". Transmission of confidential information by fax should only happen when absolutely necessary. The number / address to which it is being sent should be carefully checked beforehand.
Breaches of confidentiality	
Necessary breach of confidentiality	We recognise that occasions may arise where individual volunteers, trustees of employees feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies e.g. police or social services on a need-to-know basis.
Specific risks	If a volunteer or employee is put under pressure to disclose confidential service user information by a parent, support worker, mental health professional etc. it should be reported to the CEO or one of the trustees within 24 hours using emergency contact details (either the Battle Scars mobile phone or the CEO's)
Policy review	
Responsibility	It is the responsibility of the CEO to review this policy unless the task has been delegated to an appropriate volunteer or employee before the policy review date.
Procedure	All volunteers and employees can have input in this policy's review via their supervision.
Timing	The review must be completed within a month of the review date.