BATTLE SCARS CIO DATA PROTECTION 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 Debbie Riley – trustee
Date approved by Board	31/01/20
Reviewed	02/01/20
Amended	Yes
Policy review date	31/01/22 Every 2 years or earlier if required to match up current legislation.
Distributing	This policy will be available on the Battle Scars website and staff shared drive. 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.
Introduction	
Purpose of Policy	To: • comply with the law and the General Data Protection Regulation (GDPR); • follow good practice; • protect service users, volunteers, trustees, members and employees; • protect the organisation.
Controller	The Data Controller is the legal 'person' responsible for complying with the Data Protection Act. It is the organisation, not an individual staff member or volunteer.
Data Subject	The person the data is about.
Subject access	Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request, the Data Controller must provide a permanent, intelligible copy of the personal data about the Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third party" means either that the data is about someone else, or someone else is the source.) *See Subject Access section below*

Personal data	Considered as personal data: • full names of service users & volunteers; • full addresses of service users, volunteers, members, trustees & employees; • contact details (telephone numbers and email addresses) of service users, volunteers, members & trustees; • employees' personal contact details (i.e. not work email address and phone number); • dates of birth / ages of service users, volunteers, members, trustees & employees; • details of service users', volunteers', trustees' & employees' physical and/or mental health; • specific details of logged experiences with Battle Scars which could identify the person logging the experience (e.g. date, location and services used) • employee National Insurance and bank details; • bank details held for the reimbursement of expenses. Not considered as personal data: • first part of service users' address post codes.
Policy statement	A commitment to: • comply with both the law and good practice; • respect individuals' rights; • be open and honest with individuals whose data is held; • provide training and support to volunteers, employees and trustees who handle personal data, so that they can act confidently and consistently.
Key risks	• Information about individuals getting into the wrong hands, through inappropriate disclosure of information or poor security; • individuals being put at risk or harmed through data being inaccurate or insufficient (e.g. volunteers not receiving the right level of support due to insufficient data regarding their health).
Responsibilities	
Trustees	The trustees have the overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	Jenny Groves - CEO Responsibilities include: • briefing the trustees on Data Protection responsibilities; • Data Protection compliance and review of Data Protection and related polices; • advising volunteers and employees on tricky Data Protection issues; • ensuring that Data Protection induction and training takes place; • check if registration (notification) with ICO is required; • handling subject access requests; • approving unusual or controversial disclosures of personal data.
Specific others	Any trustee / volunteer / staff who has access to the Battle Scars IT equipment or paper records.
Team managers	N/A

Everybody doing work for Battle Scars	All trustees and employees are required to read, understand and accept any policies that relate to the personal data they may handle in the course of their work. Volunteers will be given a summary of this policy. Training will be provided if they handle personal data as part of their role.
Enforcement	Formal warning will be the penalty for infringing the Data Protection and related polices. Dismissal will be the penalty for repeatedly infringing the Data Protection and related polices.
Confidentiality	
Scope	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.
Understanding of confidentiality	*See Confidentiality 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.
Communication with Data Subjects	• The confidentiality rule in the group agreement is explained to all new service users. • Clear indicators on how we will use logged experiences data are on both the paper and the on-line form as well as the option to provide permission for follow up contact.
Communication with volunteers & staff	All volunteers and employees will receive training on how to treat disclosed information with clear procedures, ongoing support and supervision.
Communication with members	All data we request is clearly stated on the membership form. No other data is required from members.
Authorisation for disclosures not directly related to the reason why data is held	Disclosures: • if they are at the instigation or in the interest of the Data Subject, consent from the Data Subject will be the normal authorisation; • made in the course of official investigations. It may be appropriate for the Data Subject not to be informed. The CEO or chair of the board of trustees will authorise such a disclosure.
Security	
Scope	Confidentiality is about setting the boundary – defining what is allowed. Security is about ensuring the boundary is maintained.
Setting security levels	Volunteers and employees 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	• 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. • Confidential information must not be stored on pen/flash drives. Such information must be held on a separate hard drive. This drive must not be connected to any IT equipment while it is connected to the internet.
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)
Data breach	• In the event of a data breach the board of trustees will be informed. We will also inform relevant authorities within 72 hours, giving full details of the breach and proposals for mitigating its effects. • If registered with ICO data breeches of certain types of data where it's likely to result in a risk to the rights and freedom of individuals will be reported. • Depending on the data, those concerned may be notified directly.
Data recording and storage	
Type of data held	• New group attendee surveys with name, optional age and contact number and information regarding the reasons for attendance. • Membership form information. • Training feedback. • Complaints. • Safeguarding. • Logged experience information. • Volunteer application information. • Paid position application information. • Opting-in forms and emails for mail-outs. • Other data related to our services.
Transferred data	Out of data gathered by the Battle Scars Unincorporated Association (community group) only data where consent was obtained from the Data Subject was transferred to Battle Scars CIO. All other statistical data has been transferred with all personal information removed making identification of the Data Subject impossible.
Accuracy	All data is provided by the Data Subject and no personal data is shared with agencies or individuals outside of Battle Scars. • The information is received via email, on-line submissions or on hard copy either posted or handed in (such as membership forms and new service user surveys filled in at the groups). This data is considered accurate as it's made by the person supplying it. The majority of data collected is for statistical purposes.

	• Anonymous feedback collected following training and at similar events is accepted on face value and is for statistical purposes and will be used for the improvement of services. • Complaints and safeguarding concerns / reports / allegations will be investigated to determine accuracy (either by Battle Scars or by the relevant authorities).
Updating	• There is no requirement to update personal data. • If data relates to Battle Scars membership the personal data will be considered accurate unless the member provides us with updated data during their membership. • Data held for mail out purposes will be checked and updated if an email to a service, an individual or an organisation is undeliverable.
Storage	Data is held on the CEO's and/or the Battle Scars laptops, both password, PIN or fingerprint protected and fitted with anti-virus and anti-hacking software. The charity members register will only be stored on a computer without internet connection or an external drive. If the information is kept on an external drive the drive will be stored in a locked box or cupboard and only accessed via a computer disconnected from the internet. Personal electronic details following a safeguarding incident will be similarly kept as well as a backup of employees' financial details.
Retention periods	• New group member surveys to be kept for no longer than 2 years following the service user's last attendance. If the service user is still attending the paper surveys will continue to be kept as they hold the only contact information available which could be used to notify the service user in case of group meeting cancelation. • Paper feedback forms can be destroyed once they have been logged electronically. The electronic log will be ongoing. • Logged experience paper forms can be destroyed once they have been logged electronically. The electronic log will be ongoing. • Membership forms will be kept for the duration of the membership. Membership information will be kept on the separate hard-drive as an ongoing file. Personal details of members will be deleted within 2 years of the end of their membership. Non-identifiable information will be kept for statistical purposes. • The written records of all formal complaints will be held by the Chair of the board of trustees, including any written legal or insurance responses, and transferred to his/her successor as a strictly confidential file. An electronic log of complaints will be kept in a password protected computer / server / cloud. Hard copies will be kept in a locked box / cupboard. All recorded information regarding complaints will be kept for a minimum of 10 years. • Mail-out opting in forms / website entry emails can be destroyed / deleted once the date and method of consent have been recorded in the database.

	• Postal and email votes counted by the scrutineers must be stored following the official results. Depending on what the voting was for they must be kept for the periods below:
	  ○ Trustee votes until the next AGM.
	  ○ Amendments to constitution votes must be stored with the relevant minutes.
	  ○ Dissolution of the organisation votes can be destroyed after the Charity Commission has confirmed receipt of the decision.
	• Safeguarding incident forms and all written records relating to the incident will be kept by the CEO or chair of the board of trustees while the case is open. Once the case is closed, they will be held by the chair of the board of trustees and transferred to his/her successor as a strictly confidential file. All electronic records will be kept in a password protected computer / server / cloud. Hard copies will be kept in a locked box / cupboard. All recorded information regarding safeguarding children must be kept at least until the subject is 22 years old. Information regarding safeguarding adults should not be destroyed.
	• Successful application forms and references for volunteer positions will be kept in the volunteer files. These will be archived if they no longer volunteer for Battle Scars.
	• Successful application forms and references for paid posts will be kept in the employee files. If their employment comes to an end they will be archived.
	• Unsuccessful applications for volunteer and paid positions will be destroyed following the selection process.

Archiving	• Data no longer used will be archived or deleted. • Archived data will be destroyed three years after being archived.
Subject access	
Responsibility	Any subject access requests will be handled within the legal time limit of one month. The Data Protection Officer is responsible for processing such requests.
Procedure for making a request	Subject access requests can be in writing (paper or email) or verbal. If such a request is received by a volunteer, they need to pass it on to the volunteer leader / manager, the CEO or a trustee within 5 working days.
Lawful basis	The lawful basis will be explained when responding to a subject access request *(see Lawful Bases for processing below).*
Granting access	We can refuse requests that are manifestly unfounded or excessive. If we refuse a request, we will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We will do this without undue delay and at the latest, within one month.
Provision for verifying identity	If the person managing the access procedure does not know the individual personally, they will need to check their identity before handing over any information.
Provision for granting access	The required information will be provided in “permanent form” (printed on paper) unless the person requesting is happy to have it emailed or read it out to by the person managing the access procedure but it will be offered to be printed and posted or

	emailed. The information will be provided in an easy to understand manner and in clear language.
Transparency	
Commitment	We hold data for: • statistical purposes; • mail-out purposes; • networking purposes; • complaints; • safeguarding issues; • employee records; • volunteer records; • the facilitation of service improvement; • reporting incidents of good or bad practice which have been logged with Battle Scars to relevant organisations and panels (third sector or NHS). The identity of the Data Subject will remain confidential unless they wish to be identified. If the Data Subject has indicated they are happy to receive further contact any such contact will come from Battle Scars only.
Procedure	Data Subjects will be informed of transparency as required via: • clear statements on forms; • clear statements on the website.
Responsibility	The CEO has the overall responsibility for transparency.
Lawful bases for processing	
Importance of lawful bases and different types	Under the GDPR the first principle requires that we process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if we have a lawful basis under Article 6. And to comply with the accountability principle in Article 5(2), we must be able to demonstrate that a lawful basis applies. If no lawful basis applies to our processing, our processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully. The individual's right to be informed under Article 13 and 14 requires us to provide people with information about our lawful basis for processing. We therefore include these details in our privacy notice/principles. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data: 1. Consent: the individual has given clear consent for us to process their personal data for a specific purpose. 2. Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract. 3. Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations). 4. Vital interests: the processing is necessary to protect someone's life. 5. Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

	6. Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if it's a public authority processing data to perform official tasks.)
Consent	Consent is the lawful basis for processing personal data gathered for statistical purposes, membership, mail-outs, complaints, networking and volunteering.
Contract	Contract is the lawful basis for processing personal data for paid employment contracts or supply of goods and services.
Vital Interests	Vital interests is the lawful basis for processing personal data for the safeguarding of vulnerable adults or children.
Consent	
Definition	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Underlying principles	Consent must be given freely, specifically, in an informed, unambiguous, granular, clear and concise manner. Consent will be given by a clear, positive opt-in. Withdrawal of consent is the Data Subject's right. We have simple, clear ways to withdraw consent at any time. On new service user surveys it's clearly indicated that providing personal information is optional. Only data required for a specific purpose will be collected.
Forms of consent	Consent is given when the Data Subject: • freely provides data • provides data when its provision is marked as optional • specifically gives consent (e.g. on the logging experiences form) • ticks an opt-in box Verbal consent will be accepted in certain situations. The giving of verbal consent will be documented if it's deemed important by the person dealing with the particular data.
Opting out	• When the provision of data is marked as optional the Data Subject can decide whether to provide it or not. • A service user always has the right to opt out from filling in the new member survey but the way such information will be used will be explained to them in an attempt to change the service user's mind. • Instructions on how to opt out of a mailing list are included on every such email. • It is clearly marked on membership forms which information is optional or there is a clear choice available. • The option to opt out of providing information required on the volunteer application forms is not available even though certain fields can be omitted following joint agreement between the applicant and Battle Scars. On the on-line application form the non-optional fields are clearly marked with a red asterisk. All other fields are optional. • The option to opt out of providing information required on the paid staff application or when required for an employer /

	employee relationship where the lawful basis is contract is not available.
Withdrawing consent	Consent can be withdrawn by notifying Battle Scars. Clear instructions will be easily found on forms / emails or available upon request. If consent has been withdrawn the person's details will be permanently erased (deleted on all forms of electronic storage or the paper form will be destroyed). Upon withdrawal of consent, and only if the data still needs to be used for statistical purposes, the name, age and any other personal details will be replaced with a non-related numerical or alphabetic ID or left blank and no further identification of the Data Subject will be possible.
Direct mailings	
Opting in / out	Inclusion on our mailings database can only be instigated by the Data Subjects. They can request to opt out at any point (instructions are included in such emails).
Sharing lists	Lists will not be shared as a whole. Specific contact information could be passed on to fellow organisations upon request but only if such information is readily available on the Data Subject's organisation's website or on leaflets/posters and will therefore be shared as a way to assist the fellow organisation.
Volunteer & employee training & acceptance of responsibilities	
Induction	All volunteers and employees who have access to any kind of personal data will have their responsibilities outlined during their induction. If a task involving handling of or access to personal data is added on after their induction the responsibilities will be explained before they undertake it.
Procedure for volunteers and employees signifying acceptance of policy	Employees will be asked to read all Battle Scars policies and will need to sign to confirm they have read and understood them. The Data Protection Officer will be available to answer any queries. Volunteers will be given a summary of this policy during their induction and further training will be provided if they handle data as part of their role.
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.
Registration (notification) under the Data Protection Act	
Required or not	Battle Scars are not currently required to register with ICO (Information Commissioner's Office)