Battle Scars CIO Information Technology Policy

Policy information	
Organisation	Battle Scars
Scope of policy	Applies to all staff, trustees and volunteers
Policy operational date (original)	04/01/21
Policy prepared by	Jenny Groves – CEO
Reviewed:	03/01/23
Amended	Yes
Date approved by Board	09/01/23
Policy review date	By 31/01/25 Every 2 years
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	
Statement & purpose of policy	The purpose of this policy is: • to set out the parameters on how staff, trustees and volunteers should use the technology provided to them in order to do their job; • to help raise awareness of the risks associated with using IT; • to protect Battle Scars from loss of data; • to clarify what is acceptable and non-acceptable use of IT and what will happen if this policy is breached. We have the right to monitor work use of IT equipment provided we have a legitimate reason and we inform staff we might do this.
Application	This policy applies to usage of Battle Scars computers/laptops, internet access, remote access connections, file storage, smart phones/mobile phones and tablets.
Policy	
Equipment	Each Battle Scars member of staff will be provided with a Battle Scars laptop to use when carrying out work for the charity. Some laptops will be specifically designated for volunteer use with appropriate access
Passwords	• All Battle Scars computers/laptops must be password or PIN protected as a minimum. Such passwords must not be disclosed to anybody

	• Passwords must be a minimum of 8 characters and include letters and numbers. Consecutive or repeating numbers should be avoided (e.g. 1234, 9999) • If an employee suspects someone else knows their password, they need to change it as soon as possible and notify their line manager.
Computer usage	• When laptops are not being used or the member of staff is away from their desk, the lid needs to be dropped to put the laptop to sleep and staff need to log back in upon their return. This does not apply when working from home. • We discourage staff using their own laptops when working for the charity. If used, suitable anti-virus software must be installed. If unsure, they must not be used to carry out Battle Scars work. • All work for the charity must be saved on the Battle Scars One Drive [cloud storage] (or similar) as set up by the charity. • It is recommended that staff use the Battle Scars One Drive (or similar) instead of saving personal files on the laptop's hard drive. • Usage of USB drives needs to be kept to a minimum. Providing access to the appropriate One Drive folder is advisable. • Battle Scars laptops are the responsibility of the employee or volunteer when out of Battle Scars premises.
Email	Use of email by Battle Scars employees is permitted and encouraged where such use supports the goals and objectives of the charity. Employees must ensure that they: • use email in an acceptable way • do not create unnecessary risk to the charity by misusing the email facilities *(see Misuse section below).*
Smart/mobile phones	• Staff and volunteers can use their personal phones to carry out Battle Scars work such as emails. Phones must be PIN/pattern lock protected. • Work related mobile phone texting is suitable between staff and volunteers. It is recommended that the Battle Scars phone is used if texting service users is required. • No illegal or discriminatory content is allowed *(see Misuse section below)*.
Data protection	All staff must read and follow the Battle Scars Data Protection policy. A summary of the policy is in the volunteer handbook.
Internet and social media	Employees are encouraged to use the internet to carry out their tasks. Social media work is listed as a task in some staff job descriptions and volunteer role descriptions. Personal use of social media is permitted as long as it's limited to breaks (staff). All care must be taken to avoid bringing the charity into disrepute. Views must be stated as being personal *(see Misuse section below)*.
Software	No software must be installed or downloaded onto work machines without the CEO's permission.

Misuse	The following behaviour by an employee is considered unacceptable: • distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal • distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment • use of Battle Scars communications systems to set up personal businesses or send chain letters • forwarding of Battle Scars confidential messages to external locations • accessing copyrighted information in a way that violates the copyright • breaking into the charity's or another organisation's system or unauthorised use of a password/mailbox • attempting to discover a user's password • broadcasting unsolicited personal views on social, political, religious or other non-business related matters • transmitting unsolicited commercial or advertising material • undertaking deliberate activities that waste staff effort or networked resources • knowingly introducing any form of computer virus or malware into the corporate network • attempting to circumvent the network's security • leaving laptops unattended in public places.
Consequences of misuse	Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure.
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.