Charity 501
SC501001

Cyber Security Policy

0.1 | Draft for board approval

Document Control

Document title	Cyber Security Policy
Version	0.1
Status	Draft for board approval
Owner	
Approved by (name and role)	
Date approved	
Next review due	
Classification	

Version History

Version	Date	Author	Summary of changes
0.1			

Before adoption

Confirm every field above and every placeholder in this document (such as [INSERT NAME] or [INSERT DATE]) has been completed before the board adopts it. Then read the whole document against the charity's own circumstances: every statement about what the charity holds, has decided, has arranged or has already done must be true, and anything that is not must be changed before adoption.

- [CHARITY TO CONFIRM: the name or role title of the Cyber Security Lead, and insert it into sections 1.4, 10.2 and 10.4]
- [CHARITY TO CONFIRM: the contact details for the Cyber Security Lead, and insert them into section 10.4]
- [CHARITY TO CONFIRM: our current ICO registration status, using the self-assessment tool at ico.org.uk/registration, and update the ICO Registration / Data Protection Fee Status record accordingly]
- [CHARITY TO CONFIRM: our current Cyber Essentials certification status, and insert the correct statement into section 11.2]
- [CHARITY TO CONFIRM: that MFA is currently enabled on all accounts holding personal data, and identify any accounts where it is not yet active so remediation can be planned]
- [CHARITY TO CONFIRM: that a process is in place for removing access when someone leaves, and that the Cyber Security Lead has a current list of all systems, accounts and access points to be managed]
- [CHARITY TO CONFIRM: that cyber risk appears on our risk register, or that it will be added before this policy is adopted]
- [CHARITY TO CONFIRM: that our Data Breach Reporting Procedure is in place and covers the five-stage response process this policy refers to in section 7.5]

Important: These are draft outputs from a Charity Compliance Engine advisory session. They require trustee review, adaptation to your specific circumstances, and formal board approval before adoption. They do not constitute legal advice. Independent professional advice should be sought for complex or high-risk areas.

Contents

Document Control 2
Version History 2
Before adoption 2
Contents 4
Cyber Security Policy 5
1. Purpose and Scope 5
2. Legal Framework 5
3. The Five Cyber Essentials Controls 5
4. Passwords and Authentication 6
5. Recognising and Responding to Phishing 6
6. Device Security and Acceptable Use 7
7. Personal Data Breaches and the 72-Hour Notification Duty 7
8. Handling and Storing Data Securely 8
9. When Someone Leaves — Access Removal 8
10. Responsibilities 9
11. Cyber Essentials Certification 9
12. Review 9
13. Related Policies and Documents 9
Reference Materials 11

A DIAGRAM FROM THIS POLICY

The Cyber Essentials controls

Shown in full. In the policy it sits beside the text it supports.

