Cyber Security

	Yes	Needs Attention
Are monthly backups of all business and financial information undertaken?	☐	☐
Are backups stored in a secure, off-site location?	☐	☐
If we use a cloud-based storage system, is it a reputable provider?	☐	☐
Do you have a documented Privacy Policy which details how confidential information will be collected, stored and shared?	☐	☐
Do you have a documented Data Breach Response Plan?	☐	☐
If you collect and store credit card account information on your computers, is information encrypted?	☐	☐
Are all organisational financial records password protected?	☐	☐
Are computer passwords required to be changed at least every 3 to 6 months?	☐	☐
Do you have a qualified computer support company or person to secure your computer systems?	☐	☐
Are all computer operating system updates current?	☐	☐
Do you have an up to date virus and spyware protection software installed on your systems?	☐	☐
Do you have firewall systems installed on your computer network which will prevent unauthorised access to your network?	☐	☐
If you have a free Wi-Fi system available for your members, have you created a separate, private network for the organisations administrative computers?	☐	☐
Do you restrict access to objectionable or illegal wi-fi use by blocking questionable websites, password-protecting the wireless network and asking users to agree to an Internet Usage Policy?	☐	☐
Do all electronic financial transactions require a two-step verification process before processing? (e.g security question or second signatory to approve)	☐	☐
Are all requests for changes to bank account details by suppliers checked directly with the supplier, by telephone, with a known contact prior to amending?	☐	☐
Are all staff and volunteers trained in cyber risks (e.g. how to identify suspicious communication, what to do in the event of a cyber-attack)	☐	☐
Do you have insurance in place to cover you in the event of a cyber-attack or data breach?	☐	☐