Charity Trustee Confidentiality and IT Policy

1. Purpose

The purpose of this policy is to protect the charity's data, reputation, and the privacy of our beneficiaries. In accordance with **UK GDPR** and the **Data Protection Act 2018**, all Trustees have a legal duty to handle personal data securely and maintain the confidentiality of the charity's internal affairs.

2. Confidentiality Agreement

Trustees will frequently have access to "Confidential Information," which includes but is not limited to:

- Personal data of beneficiaries, donors, staff, and volunteers.
- Financial records, budgets, and sensitive fundraising strategies.
- Minutes of meetings where private matters are discussed.

The Golden Rule: Confidential information must not be shared with anyone outside the Board of Trustees without express authorisation, even after a Trustee has resigned.

3. Use of Charity Email & Systems

To ensure compliance with GDPR and to protect the charity from data breaches, the following rules apply:

- **Dedicated Email Accounts:** Trustees must use their provided Children's World email address for all charity-related correspondence.
- **No Personal Emails:** Personal email accounts (e.g., Gmail, Hotmail) must **not** be used to send or receive charity business. Personal accounts lack the security oversight required for GDPR compliance.
- **No Auto-Forwarding:** Do not set up automatic forwarding from your charity email to a personal email address.
- **Security:** Multi-Factor Authentication (MFA) must be enabled on all charity accounts where available.

4. Device Security & Storage

- **Cloud Storage:** Use the charity's official cloud storage (e.g., SharePoint, Google Drive) rather than saving files locally to your desktop or a USB stick.
- **Device Locking:** If accessing charity emails on a personal phone or laptop, the device must be password/biometric protected and must not be left unattended while logged in.
- **Public Wi-Fi:** Avoid accessing sensitive charity data over unsecured public Wi-Fi networks unless using a VPN (Virtual Private Network)

5. Use of Social Media

As a Trustee, your online presence can reflect directly on the charity's reputation. To protect both the charity and your own position, the following rules apply:

5.1 Professional Boundaries

- **Personal vs. Professional:** While Trustees are encouraged to share the charity's public posts, you must not use your personal social media accounts to conduct official charity business or respond to formal inquiries.
- **Representing the Board:** Unless specifically authorized by the Chair or the Board, Trustees should not post content that claims to represent the official view of the charity.

- **Disclaimers:** If your social media profile identifies you as a Trustee, it is best practice to include a disclaimer such as: *"All views are my own and do not necessarily reflect those of [Charity Name].*

5.2 Confidentiality & Privacy (GDPR)

- **Private Information:** Never post internal board discussions, sensitive financial data, or upcoming strategic plans that have not been made public.
- **Beneficiary Privacy:** Do not post photos or names of beneficiaries, staff, or volunteers without explicit, written **GDPR-compliant consent**.
- **Tagging & Location:** Be cautious when "checking in" to private charity locations (like a domestic abuse shelter or a private board meeting) as this can inadvertently reveal confidential information.

5.3 Respect & Reputation

- **Defamation & Tone:** Trustees must not engage in online arguments, use offensive language, or make defamatory statements about partners, donors, or competitors that could bring the charity into disrepute.
- **Political Neutrality:** If the charity is a registered entity, it must remain politically neutral. Trustees should be mindful that highly partisan posts on their personal accounts may impact the charity's perceived neutrality.

Key Rule: If you wouldn't say it in a formal press release or at a public AGM, don't post it on social media.

6. Data Breaches

Under GDPR, the charity has a legal obligation to report certain types of data breaches to the Information Commissioner's Office (ICO) within **72 hours**.

Note: If you suspect you have lost a device, sent an email to the wrong person, or your account has been compromised, you must notify the Data Protection Lead immediately.

7. Return of Information

Upon ceasing to be a Trustee, individuals must:

1. Hand over or delete all digital files belonging to the charity.
2. Securely shred any hard-copy documents.
3. Cease using the charity email address (the account will be deactivated).

8. Monitoring and Review

- The Board will review trustee appointments annually to ensure diversity and skills balance.
- This policy will be reviewed every two years, or sooner if required by law or circumstance.

9. Related Policies

- Trustee Code of Conduct
- Trustee Conflicts of Interest Policy
- Safeguarding and safeguarding vulnerable adults Policy
- Subject Access Request Policy

Policy Governance & Control This policy is reviewed annually to ensure it remains compliant with current UK legislation and best practices for the charity sector.

Approved by Catherine Busby – Chair of Trustees.
Date Written: This policy was written on 11/03/2026

Next Review Date: 11th March 2027