Donor Data Security Checklist

Use this as a quick quarterly check. If you can check most items, you are in good shape.

This document was created by 4aGoodCause.

1) Accounts and logins

- Everyone has their **own login** (no shared accounts).
- **2FA is on** for all users.
- Staff use **strong, unique passwords** (a password manager helps).
- Old staff, volunteers, and vendors have been **removed the same day** they leave.
- You review the user list **once per quarter** and remove access people do not need.
- Admin access is limited to **only the few people who truly need it**.

2) Permissions (who can see what)

- Each role only has access to what they need to do their job.
- Sensitive areas (exports, payment settings, integrations, refunds) are limited to trusted users.
- You know who can **export donor data** right now.

3) Email and phishing (biggest real-world risk)

- Staff know: **Do not click "urgent" links** asking to log in or reset a password.
- Any request to change bank details, payout info, or admin access gets verified by a **second method** (phone call or new email thread).
- Password reset emails are treated as suspicious unless the user requested them.
- You use a shared rule: **"When in doubt, do not reply. Verify first."**

4) Fraud and chargebacks (protect your money and your time)

- You have one person (or a small group) who approves refunds.
- You watch for **refund fraud**: a "donor" gives using a stolen card, then asks for a **refund by check, ACH, wire, or to a different name**.
- Refunds go back to the **original payment method** whenever possible (not a check to a new address).

This checklist was created by 4aGoodCause.

- Large or unusual gifts get a quick review (name, email, location, timing, and any odd notes).
- You know where to find chargeback notices (processor emails, merchant portal, or finance inbox).

5) Donation page spam and bots

- Your donation pages have **anti-spam / bot protection** turned on (CAPTCHA or invisible bot checks).
- You watch for patterns like repeated small gifts, odd names, or many gifts from the same device or location.
- Staff know how to flag suspicious donations for review.
- Turn on your **fraud detection suite** (address checks, velocity limits, risk rules, and suspicious payment alerts).

6) Exports, spreadsheets, and files

- You only export donor lists when you truly need to.
- Export files are stored in a **restricted folder** (not “anyone with the link”).
- Exports have a **delete-by date** (example: delete within 7 to 30 days).

7) Devices and basic hygiene

- Staff devices have **auto-updates on** (computer and phone).
- Everyone uses a **screen lock** (PIN, password, or biometrics).
- Work accounts are not left signed in on shared computers.
- Staff avoid logging in to donor tools on public Wi-Fi (or use a trusted hotspot).

8) Vendors, tools, and integrations

- You have a list of tools that store donor data (fundraising, CRM, email, event tools, and accounting).
- You have removed integrations you no longer use.
- You know who has admin access in each tool.
- You only give vendors access when needed, and you set a reminder to remove it.

This checklist was created by 4aGoodCause.

9) If something seems wrong (simple response plan)

- Your team knows who to tell first (one internal point person).
- You know how to quickly: disable a user or reset passwords.
- You document the basics (what happened, when, who was affected, what you changed).
- You know how to contact your key vendors for help (fundraising platform, CRM, payment processor, email provider).

10) Quick "pass/fail" check (takes 30 seconds)

- Could a former staff member still log in today?
- Could someone export your full donor list without anyone noticing?
- Would your team recognize a fake "account locked" email?
- Would your team spot a "refund by check" request that does not match the original payment?