GoFundraise PCI DSS Responsibility Matrix

PCI DSS Area	Payment Gateway	GoFundraise	Beneficiary
1. Secure network	Secure payment processing infrastructure	Secure GoFundraise platform, hosting & integrations	Internal networks, Wi-Fi, firewalls, and internet access
2. Secure configurations	System hardening for payment platforms	Secure configuration of GoFundraise systems	Secure configuration of staff devices, browsers, and MFA
3. Protect stored card data	Storage and protection of card data (if applicable)	Does not store card data; tokenised data only	Must not store card data in emails, files, CRM notes, or messaging tools
4. Encryption of data in transit	TLS encryption for payment traffic	TLS for all GoFundraise traffic	Safe use of networks when accessing the platform
5. Malware protection	Malware controls on payment systems	Malware protection on GoFundraise servers	Endpoint protection on staff devices
6. Patch management	Patching of payment systems	Patching of GoFundraise infrastructure and software	Patching of internal devices and applications
7. Access control	Access controls to payment dashboards	Role-based access within GoFundraise	Restrict which staff can access fundraising and donor data
8. Authentication	MFA and authentication controls	Supports secure authentication and MFA	Enforce strong passwords and MFA for staff users
9. Physical security	Datacentre/cloud physical security	Datacentre/cloud physical security	Physical security of offices and workspaces
10. Logging & monitoring	Transaction and security logging	Platform and integration logging	Internal monitoring of staff activity and security events
11. Security testing	Regular penetration testing	Penetration testing and vulnerability scans	Security testing of the organisation's own systems
12. Governance & policy	PCI DSS compliance and attestations	PCI-aligned policies for the GoFundraise service	Internal security policies and vendor management

Last reveiwed: 20/03/2026