Protecting Your Charity in a Digital World

Real-world risks, practical conversations and simple steps forward

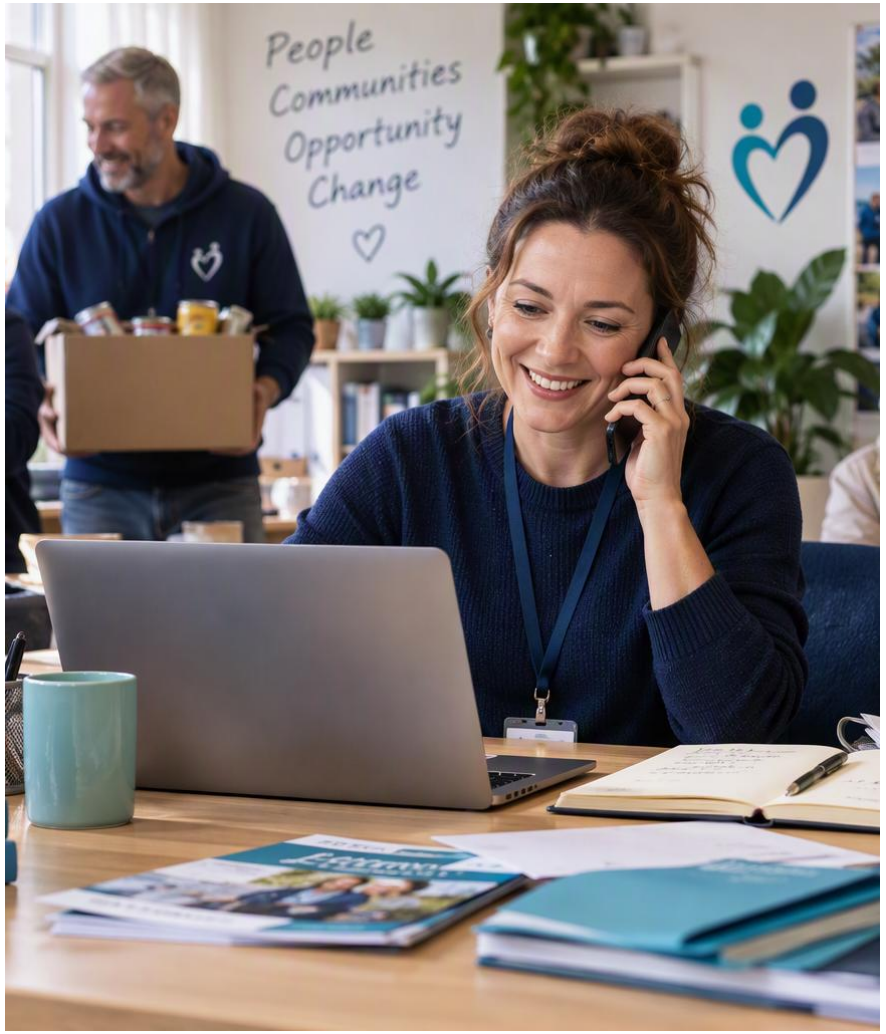
James Pinnock | Mark Le Page



Charities already depend on technology

Technology sits quietly behind the work your organisation does every day.

1. **Communicate** staff, volunteers and supporters
2. **Administer** people, services and records
3. **Fundraise** donations, campaigns and payments
4. **Safeguard** personal and sensitive information



If email or a key system stopped tomorrow, what would become difficult first?

What could go wrong?

Most incidents begin with an ordinary action on an ordinary day.



A convincing message	Someone shares a password or approves a payment.
Information goes astray	Sensitive data reaches the wrong person.
Access lingers	A former colleague or volunteer can still sign in.
Important files disappear	Records cannot be found or opened when needed.

Which scenario would have the greatest impact on your organisation?

The challenge is not just technology

Risk grows where limited capacity, unclear ownership and everyday work meet.

SMALL TEAMS	**Many responsibilities sit with a few people.**
COMPETING PRIORITIES	**Frontline needs understandably come first.**
MIXED WORKFORCE	**Staff, volunteers and trustees use the same information.**
UNCLEAR OWNERSHIP	**It is not always obvious who should act.**



The first barrier is often knowing where to begin.

The impact reaches beyond the screen

A digital problem quickly becomes a people, service and reputation problem.



TIME

Teams diverted from their purpose

SERVICE

Fundraising or support interrupted

COST

Recovery and investigation

TRUST

Confidence damaged

Which consequence would be hardest to manage?

Four simple questions

You do not need technical expertise to ask the right questions.

01	**WHAT do we rely on?**	Systems, information and services
02	**WHERE is it stored?**	Approved organisational locations
03	**WHO can access it?**	Staff, volunteers, trustees and partners
04	**WHO do we call?**	A clear route when something goes wrong

If one answer is unclear, that is a useful place to start.



Build everyday resilience

Good practice should be simple enough to become part of normal work.



- **Make ownership clear** — Name the person or group responsible.
- **Review access** — Especially when roles change or people leave.
- **Pause and question** — Check unusual requests before acting.
- **Keep a simple plan** — Know who decides, calls and communicates.
- **Talk about risk** — Include it in trustee and leadership conversations.

What is one realistic improvement you could make in the next three months?

Open discussion

What are you seeing in your charity?

- What makes good practice difficult?
- How do you balance safety and ease of use?
- How involved are trustees?
- What support would make the greatest difference?

Know what matters. Understand the risk.
Know where support is available.

