

BESPOKE

IT SOLUTIONS LTD

IT Made Simple

A practical guide for charity and non-profit
Trustees



IT Made Simple

A practical guide for charity and non-profit trustees

Protecting your people, your data and your ability to deliver your mission

Important: This guide provides general information for organisations in England and Wales. It is not legal, regulatory or insurance advice. Trustees should check current Charity Commission, ICO, NCSC, Microsoft and professional guidance when making decisions.

Bespoke IT Solutions' brand guidance calls for a warm, human and reassuring tone, with complex technology explained simply and without fear-based language.¹ This guide follows that approach: **clear questions, sensible controls and practical next steps — without expecting trustees to become IT experts.**

Set direction

Decide what good IT governance should look like for your charity.

Ask for evidence

Do not rely only on "we think it is covered". Ask how protection is checked.

Be ready

Know how the charity will continue operating and respond if something goes wrong.

The five most important actions

1. **Give one trustee or committee clear oversight of IT, cyber and digital risk.** This does not remove the collective responsibility of the board.
2. **Know which systems, services and information matter most.**
3. **Ask whether accounts, devices, data and backups are properly protected.**
4. **Approve simple policies for cyber security, data, AI, acceptable use and incidents.**
5. **Review evidence regularly:** access reports, training, backup tests, supplier performance, risks, incidents, licences and planned investment.

Trustees are providing **oversight**, not running the helpdesk. The following cycle shows what proportionate oversight can look like.

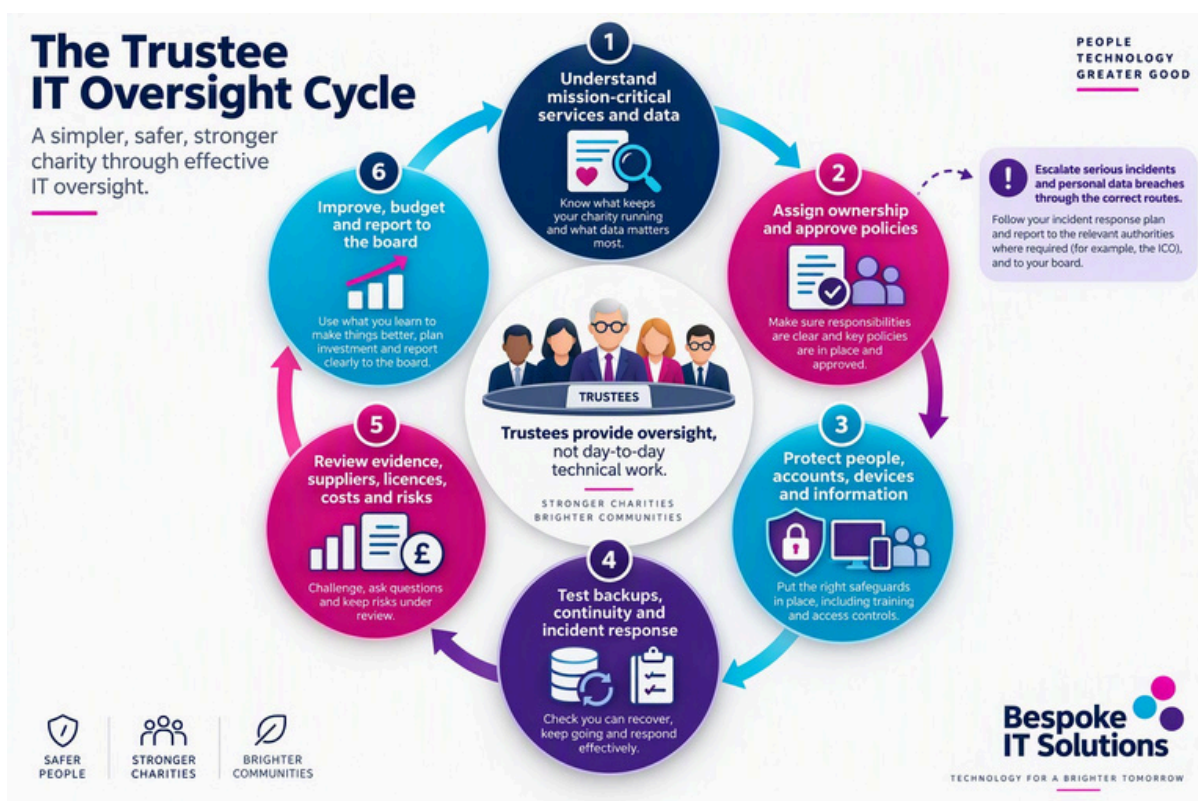


Figure 1: Trustees do not need to run IT day to day. Their role is to set direction, ask for evidence, test readiness and ensure the charity keeps improving.

1. Your responsibility as a trustee

The Charity Commission's [The essential trustee: what you need to know, what you need to do \(CC3\)](#) should be the guide's regulatory starting point.

IT should be considered wherever it affects:

- ☐ delivery of charitable services;
- ☐ protection of money, information and other assets;
- ☐ safeguarding;
- ☐ legal and regulatory compliance;
- ☐ financial controls;
- ☐ staff and volunteer safety;
- ☐ operational resilience; and
- ☐ public, donor and beneficiary trust.

What trustees should do

- ☐ **Understand:** Which activities would stop if email, phones, case-management systems, fundraising platforms or files were unavailable?
- ☐ **Assign:** Who owns day-to-day IT, cyber security, data protection and incident management?
- ☐ **Question:** What are the most significant risks, and what evidence shows they are being managed?
- ☐ **Resource:** Is the organisation providing enough money, time, training and expertise?
- ☐ **Record:** Are board decisions, accepted risks and agreed actions documented?
- ☐ **Review:** Are trustees receiving concise, understandable reports?

Requirement or good practice?

Area	Position
Acting in the charity's best interests, managing resources responsibly and complying with applicable law	Trustee duty — confirm against current Charity Commission guidance
Protecting personal information	Legal responsibility under applicable data-protection law
Reporting qualifying personal-data breaches to the ICO	Regulatory requirement where the reporting threshold is met
Reporting a serious incident to the Charity Commission	Required where the Commission's serious-incident criteria are met
Holding Cyber Essentials	Recommended assurance, not universally mandatory
Quarterly cyber reporting to trustees	Recommended good practice, not a universal legal timetable
Annual policy and continuity review	Recommended baseline; review sooner after incidents or substantial change

Use the Charity Commission's current [serious incident reporting guidance and online form](#) rather than assuming every IT fault is reportable.

2. Cybersecurity: what trustees need to know

Cybersecurity simply means protecting your accounts, devices, systems and information from loss, misuse, unauthorised access or disruption.

The NCSC's Cyber Essentials foundation covers secure configuration, security updates, access control, malware protection and internet-facing security. Bespoke's existing cyber guide sensibly adds identity, information, email, people, suppliers, backups and incident readiness.[2](#)

A sensible trustee baseline

Protect accounts

- ☐ Give each person their own account.
- ☐ Use **multi-factor authentication (MFA)** — an extra sign-in check in addition to a password.
- ☐ Restrict administrator access.
- ☐ Remove access promptly when somebody leaves or changes role.
- ☐ Review volunteer, trustee, supplier and guest accounts.

Protect devices and email

- ☐ Keep software and devices supported and updated.
- ☐ Encrypt laptops and mobile devices.
- ☐ Use automatic screen locks.
- ☐ Ensure lost devices can be managed or wiped.
- ☐ Put suitable phishing, impersonation and malware protection around email.

Bespoke's internal checklist also recommends individual accounts, MFA for cloud and privileged access, separate administrator accounts and prompt joiner, mover and leaver actions.[2](#)

Protect information

- ☐ Store charity information only in approved locations.
- ☐ Restrict access to people who genuinely need it.
- ☐ Set rules for sharing, retention and secure disposal.
- ☐ Independently verify changes to bank details or payment instructions.
- ☐ Regularly review external sharing and old guest access.

Make recovery real

A backup is a separate recoverable copy of important information. Trustees should ask:

- ☐ What is backed up?
- ☐ How frequently?
- ☐ Could an attacker delete or encrypt the backups?
- ☐ When was a restoration last tested?
- ☐ How long would critical services take to recover?

A successful backup message is not enough. The organisation should test whether priority information and services can actually be restored.[2](#)

Prepare for incidents

Keep a short plan containing:

- ☐ who leads the response;
- ☐ IT provider and insurer contact details;
- ☐ which systems or accounts should be secured first;
- ☐ an offline copy of essential contacts;
- ☐ internal and external communication routes;

- routes to the ICO, Charity Commission, NCSC or law enforcement where applicable; and
- who is authorised to make urgent decisions.

The existing Bespoke incident process illustrates useful disciplines: identify an owner, record the risk assessment, investigation, cause, actions, evidence and lessons learned, and route phishing reports through an easy staff process.[3](#)

Questions for management or the IT provider

1. Is MFA enabled for every suitable account, especially administrators?
2. Which unsupported systems or devices remain?
3. When were backups last restored successfully?
4. How quickly are leavers' accounts disabled?
5. Who monitors security alerts?
6. What happens when somebody reports a suspicious email?
7. Which suppliers can access our systems or information?
8. Have we practised our incident plan?
9. What are the three most significant cyber risks?
10. What actions need trustee support or funding?

Useful technical resources are the [NCSC Small Charity Guide](#), [Small Business Guide](#), [Board Toolkit](#) and [Cyber Essentials](#). These resources are also listed in Bespoke's current cyber guide.[2](#)

3. Safe and responsible AI

Artificial intelligence (AI) is software that recognises patterns, predicts outcomes or creates content. **Generative AI** produces new text, images, summaries or other material in response to instructions.

Appropriate charity use cases

Lower-risk examples may include:

- ☐ drafting a first version of routine communications;
- ☐ summarising non-sensitive documents;
- ☐ preparing meeting notes for human review;
- ☐ creating alternative wording or accessible versions;
- ☐ organising ideas for campaigns;
- ☐ helping staff find information in approved internal material; and
- ☐ producing first drafts of procedures or training content.

AI tools can produce convincing but inaccurate information, expose confidential data or reflect bias. Human responsibility does not transfer to the software. Internal guidance already used within Bespoke and UNISON stresses approved tools, protection of data, output validation and continued human accountability.[4](#) [5](#)

Avoid or escalate

Trustees should expect additional assessment before AI is used for:

- ☐ safeguarding decisions;
- ☐ eligibility for services or grants;
- ☐ recruitment or disciplinary decisions;
- ☐ health, care or legal advice;
- ☐ profiling beneficiaries;
- ☐ automated decisions with significant effects;
- ☐ processing special-category or highly sensitive information; or
- ☐ producing public claims without fact-checking.

A simple trustee decision framework

Before approving an AI use, ask:

1. **Purpose:** What problem are we solving?
2. **Necessity:** Could a simpler process or ordinary automation solve it?
3. **Information:** What will be entered into the tool?
4. **Approval:** Is it an organisation-approved service?
5. **Accuracy:** Who checks the output?
6. **Impact:** Could an error harm a person, service or decision?
7. **Fairness:** Could the output disadvantage particular people?
8. **Transparency:** Should people be told AI was involved?
9. **Exit:** Can the charity stop using it or correct the outcome?
10. **Evidence:** How will value, errors and complaints be monitored?

For higher-risk processing, seek data-protection advice and consider whether a **Data Protection Impact Assessment** is appropriate. A DPIA records the processing, affected people, information involved, risks, safeguards, owners and review arrangements; an internal Microsoft 365 example follows this structure.[6](#)

Useful official starting points:

- ☐ [ICO AI guidance](#)
- ☐ [UK Government AI guidance](#)

- [Data protection impact assessments](#)
-

4. Automation in charities

Automation means using software to complete a repeatable task according to set rules. It is not necessarily AI.

Examples include:

- sending acknowledgement emails after a form is submitted;
- reminding managers to review volunteer access;
- routing invoices for approval;
- notifying staff when training is due;
- creating standard folders for a new project;
- copying approved form data into a central register; and
- removing routine access when a leaver process is completed.

Automate appropriately before adding AI

1. Map the current process.
2. Remove unnecessary steps.
3. Confirm the information is accurate.
4. Decide who approves exceptions.
5. Automate the stable, repeatable part.
6. Add AI only where judgement-support or unstructured information justifies it.
7. Keep a human review for sensitive decisions.

The Bespoke AI material reinforces this approach: adding AI to a broken process can compound problems, while small pilots, oversight and measurable outcomes provide a safer route.[7](#)

5. Microsoft licensing for charities

Eligible organisations may be able to access Microsoft nonprofit grants or discounts. However, **eligibility, products, prices, seat limits and terms can change**. Check Microsoft's current [Nonprofits offers page](#) before publishing any prices or making a budget decision.

Trustees do not need to select licences

They should ask for assurance that:

- ☐ eligibility has been confirmed and retained;
- ☐ licences are matched to roles, not given out identically;
- ☐ volunteers and occasional users have an appropriate option;
- ☐ staff with greater security needs have suitable protection;
- ☐ unused licences and dormant accounts are removed;
- ☐ paid subscriptions, renewal dates and contract terms are understood;
- ☐ security features included in licences are actually configured; and
- ☐ licence changes will not unexpectedly remove protection.

Bespoke's charity material recommends role-based licence planning rather than putting everyone on the same subscription or paying for unused functionality.⁸ Microsoft capability also depends on the combination of licence, configuration and operational ownership, not simply owning a product.²

6. Staff and volunteer digital safety

A supportive culture is more effective than blaming people.

Give everyone simple instructions

- ☐ Pause when a message creates urgency, fear or excitement.
- ☐ Verify payment, password and bank-detail requests through a separate trusted channel.
- ☐ Report suspicious messages immediately.
- ☐ Never share passwords.
- ☐ Use approved storage and communication tools.
- ☐ Lock devices when unattended.
- ☐ Avoid discussing sensitive cases in public spaces.
- ☐ Report lost devices quickly.
- ☐ Do not use unapproved AI, file-sharing or messaging services for charity work.

Remote and personal devices

The charity should decide:

- ☐ whether personal devices are allowed;
- ☐ what information may be accessed;
- ☐ whether downloading is permitted;
- ☐ whether devices require encryption, updates and screen locks;
- ☐ how access can be removed; and
- ☐ what support is available.

Joiners, movers and leavers

Use a checklist covering accounts, permissions, devices, shared mailboxes, building access, password managers, third-party systems and return of equipment. This should apply to trustees, contractors and volunteers as well as employees.

7. Core policies and procedures

Document	Purpose	Suggested owner	Recommended review
IT and information-security policy	Sets overall expectations and responsibilities	Senior operational lead	Annually and after major change
Acceptable-use policy	Explains safe use of devices, email, internet and cloud services	HR/operations with IT	Annually
Data-protection and retention policy	Governs collection, access, sharing, keeping and disposal	Data-protection lead	Annually or when law/process changes
Access-control procedure	Covers account approval, permissions and administrator access	IT lead/provider	Regular access reviews
Joiner, mover and leaver procedure	Ensures access follows a person's role	HR plus IT	After process failures or system changes
AI-use policy	Defines approved tools, prohibited information and human review	Senior management/data lead	Frequently while guidance evolves
Incident-response plan	Sets contacts, authority, reporting and communication	Senior incident owner	Test at least annually
Backup and recovery procedure	Defines coverage, protection and restoration testing	IT lead/provider	After tests or system changes
Business-continuity plan	Keeps essential services operating during disruption	Senior management	Exercise and review regularly
Personal-device/remote-working policy	Sets rules for home and mobile working	HR/IT/data lead	Annually
Supplier and cloud-service procedure	Covers selection, contracts, access and exit	Finance/procurement/IT	At procurement and renewal

These review intervals are **recommended governance baselines**, not universal statutory deadlines.

8. Additional areas trustees should include

Data protection

Know what personal information is held, why it is needed, where it is stored, who can access it and when it is deleted. Use the ICO's [data protection self-assessment tools](#) and [personal-data breach guidance](#). The ICO breach resource is included in Bespoke's authoritative cyber reference set.²

Business continuity and resilience

Prioritise services, people, premises, suppliers, communications and information. Decide acceptable downtime and practise realistic scenarios.

IT budgeting and lifecycle planning

Maintain a forward view of device replacement, licence renewals, projects, security improvements, support contracts and contingency costs. A current charity-sector IT specification obtained internally includes licensing optimisation, cyber assurance, continuity, AI readiness, sustainability and lifecycle planning as connected strategic areas.⁹

Supplier due diligence

Ask potential IT or cloud suppliers about:

- ☐ relevant experience;
- ☐ data location and subcontractors;
- ☐ security certification;
- ☐ incident notification;
- ☐ access controls;
- ☐ backup responsibilities;
- ☐ service reporting;
- ☐ business continuity;
- ☐ termination and data return; and
- ☐ ownership of administrator accounts and documentation.

Accessibility

Digital services, documents and websites should be usable by people with different access needs. Include accessibility in procurement, design, testing and staff training. Start with [Government accessibility guidance](#) and the [Web Content Accessibility Guidelines](#).

Charitable companies and Companies House

Companies House is relevant where the charity is also incorporated as a company. It deals with company registration and filing responsibilities; it does **not** regulate every charity. Use [Companies House guidance](#) alongside Charity Commission guidance where both regimes apply.

9. Annual trustee IT checklist

Mark each item **Yes, Partial, No or Unknown**.

- ☐ ☐ A trustee or committee has clear IT and cyber oversight.
- ☐ ☐ Critical services, information and suppliers are documented.
- ☐ ☐ Top IT and cyber risks appear on the risk register.
- ☐ ☐ MFA protects suitable accounts.
- ☐ ☐ Administrator and leaver access has been reviewed.
- ☐ ☐ Unsupported devices and software are known.
- ☐ ☐ Backups have been successfully restored.
- ☐ ☐ The incident plan has been exercised.
- ☐ ☐ Staff and volunteers know how to report concerns.
- ☐ ☐ Policies are current and understood.
- ☐ ☐ AI and automation use has named owners and controls.
- ☐ ☐ Microsoft and other licences have been reviewed for cost and suitability.
- ☐ ☐ Supplier access and contractual responsibilities are understood.
- ☐ ☐ Technology replacement and improvement costs are in the budget.
- ☐ ☐ Previous incidents and exercises produced completed actions.

“Unknown” is useful information. It shows where trustees need evidence, not where blame should be placed.

10. Warning signs needing attention

- ☐ Nobody can say who owns IT or cyber risk.
 - ☐ One shared administrator account is used by several people.
 - ☐ Former staff or volunteers still have access.
 - ☐ MFA is inconsistent.
 - ☐ Backups have never been restored.
 - ☐ Policies exist but staff cannot find them.
 - ☐ Trustees receive no meaningful IT reporting.
 - ☐ Personal email or storage is used for charity information.
 - ☐ Staff use unapproved AI tools with work information.
 - ☐ The IT provider controls all administrator access and documentation.
 - ☐ There is no record of devices, systems, licences or suppliers.
 - ☐ Critical contacts are available only inside the system that may fail.
 - ☐ Technology investment happens only when something breaks.
-

What to do next

During the next trustee meeting

1. Name the trustee lead and operational owner.
2. Ask the ten trustee questions in this guide.
3. Record Unknown, Partial and No answers.
4. Prioritise identity, unsupported systems, backups, sensitive information and incident readiness.
5. Give every action an owner and target date.
6. Schedule a short follow-up report based on evidence.

Good evidence may include access reports, device inventories, dated screenshots, backup-restoration results, training records, approved exceptions, incident-exercise notes and current supplier documents.²

Official resources

- ☐ [The essential trustee — Charity Commission](#)
- ☐ [Report a serious incident — Charity Commission](#)
- ☐ [Internal financial controls for charities — Charity Commission](#)
- ☐ [NCSC guidance for charities](#)
- ☐ [NCSC Board Toolkit](#)
- ☐ [Cyber Essentials](#)
- ☐ [ICO checklists for small organisations](#)
- ☐ [ICO personal-data breach guidance](#)
- ☐ [ICO AI guidance](#)
- ☐ [Microsoft offers for nonprofits](#)
- ☐ [Companies House guidance](#)

Licensing, AI guidance and regulatory reporting requirements can change. Check the linked primary source before final publication.

A friendly final thought

Good charity IT is not about buying the most technology. It is about protecting trust, keeping services available, helping people work safely and using limited funds wisely.

If trustees can see the risks, understand who owns them and review credible evidence, they are already moving the organisation in the right direction.

Bespoke IT Solutions can support charities with a straightforward IT, cyber and Microsoft 365 review — clear feedback, practical priorities and no pressure. This is consistent with Bespoke's existing charity positioning: real people, tailored support, clear guidance and a low-pressure first conversation.¹⁰