



Charity  
Compliance  
Engine™

---

## Governance Compliance Review

*Prepared by Integrity Nexus Ltd using the Charity Compliance Engine*

**Prepared for: Charity 500 (SC500001)**

**Date: 01 October 2026**

### About This Review

This review summarises a Charity Compliance Engine session facilitated by Integrity Nexus Ltd for Charity 500 (SC500001), a two-tier SCIO with twelve paid staff and around forty volunteers. It covers equality, diversity and inclusion, your response to a live phishing incident, and readiness for staff use of AI tools. It sets these against the framework your trustees agreed before the session and the documents you already hold. This review provides practical governance guidance to support your compliance development. It does not constitute legal or regulatory advice, and trustees retain responsibility for reviewing and adopting any frameworks or policies discussed.

## Session deliverables

### Drafted in full

- Equality, Diversity and Inclusion Policy (version 1.0, for board approval)

### Specified, ready to draft

- AI use policy, or a short addendum to your existing cyber security policy (approved tools, a ban on entering personal data, consumer versus enterprise accounts, volunteer coverage, and approval responsibility)
- Board resolution on interim AI use (low-risk use only until the policy is adopted)
- Personal data breach response procedure (containment, access checks, data assessment, the 72-hour ICO test, NCSC reporting, notifying individuals, trustee escalation, and post-incident review)
- Internal personal data breach log
- Data Protection Impact Assessment for any AI tool that will process personal data
- Staff and volunteer briefing on AI and phishing awareness (what must never be entered, how to recognise account types, and how to report mistakes)

### Drafted in an earlier sitting

- Employment contracts
- Discipline and appeals policy and procedure
- Fraud, bribery and financial misconduct policy
- Written Statement of Employment Particulars – Support Worker
- Grievance policy and procedure
- Safeguarding policy
- Child protection procedure
- Referral policy (Disclosure Scotland)
- Cyber security policy
- Lone working policy
- Data protection policy
- Conflicts of interest policy

## Your Compliance Picture

Your organisation is building from a solid base. You have staff and volunteer handbooks, plus twelve core documents drafted in earlier sittings that cover employment, safeguarding, PVG referral, data protection, lone working, conflicts of interest and cyber security. Of the four items your trustees agreed to add, two are already drafted (the cyber security policy and the fraud, bribery and financial misconduct policy). The social media and confidentiality policies are agreed and still to start.

This session added a complete EDI policy. It also turned two current pressures into clear plans: a possible account compromise involving sensitive health and PVG data, and the arrival of AI tools in everyday work.

The headline message is that your main exposure now lies in operation rather than paperwork. Trustees need to adopt and use what has been drafted, manage the live data incident within the statutory timescale, and set rules on AI use before habits form.

## Key Areas Covered

### Legal baseline

**Equality, diversity and inclusion (in place, subject to adoption).** Your organisation is both an employer and a service provider to children and disabled adults, so the Equality Act 2010 applies to you in both directions. It covers all nine protected characteristics and four forms of unlawful conduct: direct and indirect discrimination, harassment and victimisation. The most important duty at your scale is the anticipatory duty to make reasonable adjustments for disabled people. This means identifying barriers in activities, premises, consent arrangements and trips before anyone has to ask.

A full policy is now drafted for board adoption. One point to settle before approval: the session advised an annual review, while the draft provides for a review every two years with an annual board update. Trustees should choose one cycle and record it.

**Personal data breach response (live, plan defined).** A phishing compromise counts as a personal data breach under UK GDPR wherever personal data may have been accessed. Given the health, disability and PVG data you hold, this is significant. The critical obligation is to report to the ICO within 72 hours of first becoming aware if there is a risk to individuals. You can submit an initial report and add to it later. Every breach must also be recorded internally, whether or not it is reported. Individuals must be told directly where the risk to them is high.

The session set out the full response sequence, which now needs to be captured as a standing procedure alongside your existing data protection policy. ICO registration and payment of the data protection fee should also be confirmed at [ico.org.uk/registration](https://ico.org.uk/registration).

### Items your trustees agreed to add

**Cyber security and AI use (cyber security policy already drafted; AI rules specified).** Your cyber security policy already exists and is available for trustee review. The session extended it to cover AI tools. The key risk is that consumer AI accounts have no Article 28 data processing agreement in place, and the vendor may use what you enter to train its models. Entering participant or staff personal data into these tools would therefore be a breach.

Any AI use involving special category data needs a DPIA under UK GDPR Article 35, and your Records of Processing Activities would need updating. The NCSC's warning that AI makes phishing more convincing links directly to your current incident. Awareness training should focus on behavioural warning signs rather than spelling and grammar.

**Fraud, bribery and financial misconduct (already drafted).** This policy is already drafted and available for trustee review. It is relevant to your cash handling arrangements described at intake. The session did not revisit it.

**Social media and confidentiality (agreed, still to start).** Both policies are part of the agreed framework and were not reached in this session.

## Priority Actions

1. **Close out the phishing incident now.** Contain the account, check sign-in history and establish exactly what personal data it could reach. If there is any risk to individuals, report to the ICO using [ico.org.uk/for-organisations/report-a-breach](https://ico.org.uk/for-organisations/report-a-breach). If 72 hours have already passed, report anyway and explain the reasons for the delay. Record the incident in a breach log, forward the phishing email to [report@phishing.gov.uk](mailto:report@phishing.gov.uk), and give the board a written report.
2. **Pass an interim AI resolution at the next board meeting.** Minute a decision permitting low-risk AI use only, and tell every staff member and volunteer that no personal data may be entered into any AI tool until further notice. Then adopt the AI use addendum to your existing cyber security policy. Complete a DPIA and move to an enterprise account with a data processing agreement before any use involving personal data.
3. **Review and adopt the EDI policy.** Settle the review cycle and complete the approval block. Confirm that the complaints procedure the policy refers to exists and is available on request. Brief staff and volunteers on the policy at induction and team meetings.
4. **Review and adopt the employment documents already drafted.** Your employment contracts, Written Statement of Employment Particulars, and discipline and grievance procedures are already drafted. Given the two live employment matters, trustees should review and adopt these promptly and make sure they are applied consistently. Take independent employment advice on the live matters themselves.
5. **Have the trip consent and disclaimer form checked by an adviser.** Nobody has yet tested whether this form does what you think it does. A notice of this kind generally cannot exclude liability for death or personal injury caused by negligence. An adviser can confirm what the form can lawfully achieve and how it should be reworded, including its accessibility for disabled participants and parents, in line with your EDI policy.
6. **Start the two outstanding agreed policies.** The social media and confidentiality policies complete the framework your trustees agreed. Aim to have drafts ready for the board within the current accounting year (to 31 March 2027).
7. **Bring data protection records up to date.** Confirm your ICO registration status. Make sure your Records of Processing Activities and the appropriate policy document required for your Article 9 health data and Article 10 criminal offence data are in place and current. Update them as new tools are approved.

## Areas Considered and Not Prioritised at This Stage

As part of agreeing your framework, your trustees considered the wider compliance landscape and made deliberate decisions about what not to prioritise at this stage. That record is itself evidence of considered governance.

### Deferred items

- Financial controls policy: deferred without a stated reason.
- Public liability insurance record: deferred without a stated reason.

### Legal baseline items queried

- Reserves policy: recorded as "Considered and not prioritised". This is an open question awaiting adviser review rather than an unmet obligation.

Trustees should revisit these decisions when circumstances change, such as growth, new activities, new funding or staffing changes, since items that are proportionate to defer today may become priorities later.

## Further Support

Your companion documents from this session are your Guidance Pack, which gives full plain-English guidance on each area covered, the draft EDI policy for review and adoption, and the full session transcript. The Charity Compliance Engine remains available for ongoing compliance queries. For complex or high-risk matters, such as the live employment cases, the trip disclaimer and any data breach that may require notifying individuals, independent legal or professional advice should be sought. Integrity Nexus Ltd can provide further consultation support.

**Integrity Nexus Ltd**   
Consultancy Services

Integrity Nexus Ltd | SC837413  
Blackridge, Bathgate EH48 3SG | Scotland  
[contact@integrity-nexus.co.uk](mailto:contact@integrity-nexus.co.uk)

### Important Notice

This Governance Compliance Review was produced using the Charity Compliance Engine, an AI-supported compliance tool provided by Integrity Nexus Ltd. It provides practical governance guidance based on the charity profile and queries covered in this session. It does not constitute legal or regulatory advice. Trustees are responsible for reviewing, adapting, and formally approving any policy, framework, or recommendation before it is adopted by the organisation. For matters involving significant legal complexity or financial risk, independent professional advice should be sought.