Governance Compliance Review

Prepared by Integrity Nexus Ltd using the Charity Compliance Engine

Prepared for: Charity 501 (SC501001)

Date: 18 October 2026

About This Review

This review summarises a Charity Compliance Engine session facilitated by Integrity Nexus Ltd. It covers Charity 501's governance and compliance position as a two-tier SCIO with twelve paid staff, around forty volunteers, and services for children, vulnerable adults and people with disabilities. 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. The full plain-English guidance for each area is in your Guidance Pack. This review is the short companion to that pack.

Session deliverables

Drafted in full

- Safeguarding Policy
- Child Protection Procedure
- Adults Support and Protection Procedure
- PVG Scheme Compliance Procedure
- Referral Policy (Disclosure Scotland)
- Data Protection Policy (including the appropriate policy document for special category and criminal offence data)
- Privacy Notice (service users, participants and the public)
- Data Breach Reporting Procedure
- Record of Processing Activities (Article 30)
- Cyber Security Policy
- Social Media Policy

Specified, ready to draft

- Privacy Notice for staff and volunteers
- ICO registration / data protection fee status record
- Health and Safety Policy
- Risk Assessment Procedure

- General / Premises Risk Assessment
- Incident and Accident Reporting Procedure
- RIDDOR Compliance Procedure
- Fire Safety Risk Assessment
- Emergency Evacuation Procedure
- First Aid Provision and Procedure
- Employers' Liability Insurance Record
- Employment Contracts (incorporating the statutory written statement)
- Discipline and Appeals Policy and Procedure
- Grievance Policy and Procedure
- Trustee Register
- Trustee Declaration of Eligibility
- Conflicts of Interest Policy
- Conflicts of Interest Register
- Confidentiality Policy
- Accounting Records (money in / money out)
- Receipts and Payments Accounts
- Independent Examination arrangements
- Reserves Policy
- Fraud, Bribery and Financial Misconduct Policy (including cash-handling controls)
- OSCR Annual Return
- Annual Accounts
- Trustees' Annual Report
- Charity References on External Documents
- Serious Issues Handling and OSCR Concern Reporting
- OSCR Notification of Changes Procedure
- Trip consent and information form (redesigned without the liability disclaimer)

Your Compliance Picture

Charity 501 started from a narrow written base of a Staff Handbook and a Volunteer Handbook. Trustees agreed to build a full legal baseline and to add four further items: cyber security, social media, fraud, bribery and financial misconduct, and confidentiality. This session made substantial progress on that plan. The complete safeguarding and PVG framework, the core data protection framework, and two of the four agreed additions (cyber security and social media) are now drafted and ready for board adoption. The overall message is that your highest-risk areas now have documents. Your attention should move to adopting them, filling the named roles and placeholders, and dealing with a handful of live operational issues. Those issues are PVG confirmation for every regulated role, the minibus data breach, employment contracts, the trip disclaimer and cash handling.

Key Areas Covered

Safeguarding and PVG (legal baseline). Your youth programme, support groups and trips put children and adults at risk at the centre of your work. From 1 April 2025, PVG membership is mandatory for every regulated role, and nobody may start before membership is confirmed. There is no supervised or interim start. Membership moves to a five-year renewable term from 1 April 2026. The duty to refer to Disclosure Scotland must be met within three months of the duty arising, and trustees can be personally liable for failure to refer. The session also confirmed that a volunteer driving young people monthly is very likely in a regulated role. *Status: all five documents drafted, awaiting adoption and named leads.*

Data protection (legal baseline). You hold health data (Article 9) and PVG/criminal offence data (Article 10), so your Record of Processing Activities is a legal requirement and the 250-employee exemption does not apply. Reportable breaches must reach the ICO within 72 hours of awareness. Subject access requests have a one-month deadline. A named data protection lead is needed rather than a statutory DPO. Your ICO fee status should be checked at ico.org.uk/registration. The session also covered the minibus breach and a parent's request for a 13-year-old's support notes, where the child's own views and safeguarding input come first. *Status: policy, service-user privacy notice, breach procedure and ROPA drafted. Staff and volunteer privacy notice and ICO fee record still to draft.*

Health and safety (legal baseline). With more than five employees, a written health and safety policy is a legal requirement. In Scotland, fire safety falls under the Fire (Scotland) Act 2005, so you need to confirm with your landlord who holds the fire risk assessment. RIDDOR requires specified injuries to be reported within 10 days and over-seven-day injuries within 15 days. Employers' liability cover of at least £5 million is compulsory. *Status: nine documents specified, still to start.*

Employment (legal baseline). Every worker is owed a written statement of particulars on or before day one. Only pensions, collective agreements, additional training and the discipline and grievance note may follow, within two months. With two live matters before the board, contracts are the priority. Non-compliance with the ACAS Code can adjust tribunal awards by up to 25 per cent. *Status: contracts, discipline and grievance policies specified, still to start.*

Governance baseline (legal baseline). Trustee details must be held on OSCR Online (required since 30 June 2025), and OSCR publishes trustee names from 9 March 2026. Expanded disqualification criteria have applied to trustees and senior roles since 31 August 2025. Existing declarations should be reviewed against them alongside a Record of Removed Persons check. *Status: trustee register, declaration, conflicts policy and register specified, still to start.*

Finance and reporting (legal baseline). As a SCIO with income under £250,000, you may prepare Receipts and Payments accounts with an independent examination. The examiner's report must cite Scottish legislation and be signed by a named individual. The Trustees' Annual Report must meet Schedule 2, including a full reserves statement. From 9 March 2026, accounts are published unredacted. OSCR's Notifiable Events process ended on 1 April 2024. *Status: all items specified, still to start.*

Agreed additions. The Cyber Security Policy (built on the five Cyber Essentials controls) and the Social Media Policy are drafted. The Fraud, Bribery and Financial Misconduct Policy is specified. It should set out your cash controls: two-person counts, receipting, separation of collection from reconciliation, and monthly trustee review of bank statements. The Confidentiality Policy is specified and should also cover support notes and operational health information. *Status: two drafted, two agreed and building.*

Participation disclaimers. Under Part II of the Unfair Contract Terms Act 1977 (section 16), your trip disclaimer cannot exclude liability for death or personal injury caused by negligence. A parent

cannot waive a child's right to claim. The form should be redesigned around consent and information. *Status: still to start.*

Priority Actions

1. **Confirm PVG membership for every regulated role now.** Assess each paid and volunteer role, including the volunteer driver, using Disclosure Scotland's checker, and record the outcome. Anyone in a regulated role without confirmed membership must stop until it is confirmed. Volunteer applications are free through Volunteer Scotland Disclosure Services.
2. **Close out the minibus data breach.** If not already done, the data protection lead (or the most senior person available) should assess the breach against the 72-hour ICO deadline and report via ico.org.uk/for-organisations/report-a-breach. Consider direct notification to affected participants or their parents, and record the breach in the breach log. Replace printed health lists on trips with minimal emergency alert information.
3. **Review employment contracts before the live matters progress.** Check every current contract against the day-one statutory particulars and issue corrected statements where needed. Given the live matters, take ACAS or independent HR advice (SCVO HR support is available). Draft the Discipline and Appeals and Grievance policies next.
4. **Adopt the safeguarding and data protection drafts.** Within the next board cycle, appoint and minute the Designated Safeguarding Lead, Deputy and Data Protection Lead. Complete the placeholders, including local authority contacts, retention periods and processor contracts. Then formally adopt the eleven drafted documents and draft the staff and volunteer privacy notice.
5. **Replace the trip disclaimer before the next trip.** Remove the "at your own risk / not liable" wording and redesign the form around medical information, emergency contacts and consent. Complete a written risk assessment for each trip in advance. The session also advised trustees to confirm that their existing insurance covers day trips and volunteers.
6. **Fix cash handling and draft the fraud policy.** Separate the person who collects cash from the person who reconciles and banks it, use two-person counts with a signed count sheet, and bank promptly. Have a trustee review bank statements monthly. Record these controls, plus a safe reporting route, in the Fraud, Bribery and Financial Misconduct Policy.
7. **Secure the governance and health and safety baseline.** Confirm that trustee details are current on OSCR Online, review declarations against the expanded disqualification criteria, and check ICO registration status. Then start the Health and Safety Policy, obtain or carry out the fire risk assessment with your landlord, and record your employers' liability certificate and renewal date.

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.

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

No legal baseline items were queried.

Trustees should revisit these decisions when circumstances change (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 the Guidance Pack (the full plain-English guidance for each area covered), the eleven policy and procedure drafts for trustee review and adoption, and the full session transcript. The Charity Compliance Engine remains available for ongoing compliance queries, including drafting the specified documents listed above. For complex or high-risk matters, such as the live employment cases, the data breach or a disputed subject access request, 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

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.