



Charity
Compliance
Engine™

Integrity Nexus Ltd 
Consultancy Services

Compliance Guidance

A plain-English reference for your trustees and volunteers, prepared by Integrity Nexus Ltd using the Charity Compliance Engine

Prepared for: Charity 500 (SC5000001)

Date: 20 September 2026

This Compliance Guidance pack collects the plain-English guidance discussed during your Charity Compliance Engine session, organised by area and kept for your trustees and volunteers to refer back to. It explains why each area matters for a charity like yours, what good practice looks like at your scale, and the common pitfalls to avoid. It is a learning and reference resource: it sits alongside your Governance Compliance Review (which records decisions and next steps) and your draft policy documents (which you adopt).

Contents

Your compliance framework	5
Governance foundations	6
Trustee Register	6
Trustee Declaration of Eligibility	6
Conflicts of Interest Policy	7
Conflicts of Interest Register	7
Data protection	12
Data protection policy	12
Privacy notice	13
ICO registration / data protection fee status	13
Data breach reporting procedure	14
Record of processing activities (Article 30)	14
Health, safety and premises	18
Health and safety policy	18
Risk assessment procedure	18
General / premises risk assessment	19
Incident and accident reporting procedure	19
RIDDOR compliance procedure	19
Fire safety risk assessment	20
Emergency evacuation procedure	20
First aid provision and procedure	20
Employers liability insurance record	21
Finance and OSCR reporting	25
Accounting records (money in / money out)	25
Receipts and payments accounts	25
Independent examination	26
OSCR annual return	26
Annual accounts (appropriate format for income level)	26
Trustees' annual report	27
Charity references on external documents	27
Serious issues handling and OSCR concern reporting	27
OSCR notification of changes procedure	28
Additional guidance from your questions	32
Can you draft our fraud and financial irregularity policy	32
Participation waivers and liability disclaimers in Scotland	33
The legal position	33
What "at your own risk" actually means in practice	33
The position for children	33
What the form should actually do	33

What actually protects the charity	34
The immediate practical step	34
We are a small team. Do we really need all of these separate documents, or can some be combined?	35
What can reasonably be combined	35
What must stay separate	35
The practical consolidation path	36
The bottom line	36
We need to draft employment contracts - can you help?	37
Redundancy — process and obligations for a small Scottish charity	38
What makes a dismissal a redundancy	38
The fair process	38
Collective consultation threshold	38
Selection criteria	38
Statutory redundancy pay	39
Alternatives to redundancy	39
Recommended next steps	39
Notice periods — statutory minimums and contractual terms	40
Statutory Minimum Notice	40
Contractual Notice	40
When Notice Starts	40
Payment in Lieu and Dismissal Without Notice	40
Practical Check	40
Equality, Diversity and Inclusion Policy — Legal Requirements and Good Practice	41
Legal Foundation	41
What an EDI Policy Achieves	41
What Good Looks Like	41
Specific Considerations for Charity 500	42
Annual Review	42
Responding to a Phishing Incident and Data Breach	43
Immediate Containment	43
Check for Unauthorised Access	43
Assess What Data the Account Holds	43
The 72-Hour ICO Reporting Obligation	43
Document Everything	43
Report the Phishing Email	43
Consider Direct Notification to Affected Individuals	44
Trustee Involvement	44
ICO Registration	44
Post-Incident Review	44
AI Tools — Governance and Data Protection Readiness	47
The Core Risk	47

What Should Be in Place Before Use Begins	47
A Trustee-Level Decision	47
An AI Use Policy (or Addition to the Cyber Security Policy)	47
Data Processing Agreements	47
A Data Protection Impact Assessment	48
Staff and Volunteer Training	48
Records of Processing Activities	48
Account Security	48
The NCSC Position	48
A Practical Starting Point	48