NILO Data Protection (UK GDPR) Policy

1. Purpose and scope

NILO collects and uses personal data lawfully, fairly and securely, and only as far as its grant-making work requires. This policy sets out how NILO meets its duties under UK data protection law and what everyone working for NILO must do.

The policy applies to:

- All personal data NILO processes, in any format: digital records, email, grant management systems, spreadsheets, paper files, photos and recordings.
- Everyone who handles that data for NILO: trustees, staff, volunteers, contractors, consultants and grant assessors.
- Data about applicants, grantees, beneficiaries, donors, partners, suppliers, staff, trustees, volunteers and members of the public.

NILO is the **data controller** for the personal data it decides to collect and use. Failure to follow this policy may lead to disciplinary action for staff, or the end of an engagement for volunteers and contractors.

NILO is a registered UK charity (1195271) with Company number: 13261660.

2. Legal framework and definitions

NILO follows the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (PECR), as amended by the Data (Use and Access) Act 2025. NILO also follows guidance from the Information Commissioner's Office (ICO), the Charity Commission and the Fundraising Regulator.

Term	Meaning
Personal data	Any information about an identified or identifiable living person, such as a name, email address, ID number or opinion about them.
Special category data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation.
Criminal offence data	Data about criminal allegations, proceedings, convictions or related security measures, including DBS checks.
Processing	Anything done with personal data: collecting, recording, storing, using, sharing, deleting.
Data subject	The person the data is about.
Controller	The organisation that decides why and how data is processed (NILO).
Processor	An organisation that processes data on NILO's instructions, such as an IT or payroll provider.
Personal data breach	A security incident leading to the accidental or unlawful loss, destruction, alteration, disclosure of, or access to, personal data.

3. Data protection principles

NILO applies the seven UK GDPR principles to all processing. Personal data must be:

1. **Lawful, fair and transparent** — processed on a valid lawful basis, in ways people would reasonably expect, and explained in clear privacy notices.
2. **Purpose limited** — collected for specified purposes (for example, assessing a grant application) and not reused for unrelated purposes without a new lawful basis.
3. **Minimised** — adequate, relevant and limited to what is necessary. Application forms ask only for what assessment and due diligence need.
4. **Accurate** — kept up to date, with inaccurate data corrected or deleted promptly.
5. **Storage limited** — kept no longer than necessary, in line with NILO's retention schedule (section 10).

6. **Secure** — protected against unauthorised access, loss or damage by appropriate technical and organisational measures.
7. **Accountable** — NILO must be able to show it complies, through records of processing, policies, training, contracts and impact assessments.

4. Roles and responsibilities

The Board of Trustees is ultimately accountable for data protection at NILO; day-to-day oversight sits with a named Data Protection Lead.

Role	Responsibilities
Board of Trustees	Approves this policy; ensures adequate resources; receives an annual data protection report; decides on serious incident reports to the Charity Commission.
Data Protection Lead	First point of contact for data protection; keeps the record of processing activities; handles rights requests and breaches; advises on DPIAs; arranges training; liaises with the ICO.
Director / senior staff	Make sure their teams and systems follow this policy; build privacy into new projects and grant programmes.
Staff, volunteers and assessors	Handle personal data only as their role requires; follow this policy; complete training; report breaches and rights requests to the Data Protection Lead immediately.
Contractors and processors	Process data only on NILO's written instructions and under a data processing agreement.

NILO is not currently required to appoint a statutory Data Protection Officer, as it is not a public authority and does not carry out large-scale monitoring or large-scale processing of special category data. The Board will review this if NILO's activities change.

Open question: confirm who will act as Data Protection Lead, and whether one trustee should be the named data protection champion.

5. Whose data NILO processes and why

Most of NILO's personal data comes from grant-making: contacts at applicant and grantee organisations, and, more sensitively, information about the people grantees serve. The table below is a summary; full detail sits in NILO's Record of Processing Activities (RoPA).

Data subjects	Typical data	Main purposes	Usual lawful basis
Applicant and grantee contacts	Name, role, contact details, organisation, bank details (for payments), correspondence	Assessing applications, due diligence, making and monitoring grants, payments	Legitimate interests; contract (grant agreement)
Trustees and key people at applicant organisations	Name, role, date of birth, disqualification checks, conflicts of interest	Due diligence, fraud and safeguarding checks	Legitimate interests; legal obligation
Beneficiaries of funded work	Case studies, monitoring data, photos, quotes; sometimes health or other special category data	Grant monitoring, impact reporting, communications	Consent (case studies and images); legitimate interests (anonymised or pseudonymised monitoring)
Individual grant recipients (if any)	Contact details, circumstances, financial information, supporting evidence	Assessing eligibility and paying grants	Legitimate interests; explicit consent or substantial public interest for special category data
Donors and supporters	Name, contact details, gift history, Gift Aid declarations, preferences	Processing gifts, claiming Gift Aid, thanking and updating supporters	Contract; legal obligation (Gift Aid); consent (electronic marketing)
Partners, peers and stakeholders	Name, role, organisation, contact details	Collaboration, events, newsletters, LinkedIn and other communications	Legitimate interests; consent (electronic marketing)

Staff, volunteers, assessors and contractors	Recruitment data, contracts, payroll, HR records, emergency contacts, DBS checks where relevant	Employment and engagement, payroll, legal compliance	Contract; legal obligation; legitimate interests
Trustees	Contact details, declarations of interest, eligibility checks, Charity Commission and Companies House filings	Governance and regulatory compliance	Legal obligation; legitimate interests
Website visitors	IP address, cookies, enquiry form data	Running the website, answering enquiries	Consent (non-essential cookies); legitimate interests

Where NILO relies on legitimate interests, it keeps a documented legitimate interests assessment (LIA). Where grantees share beneficiary data with NILO, NILO asks for anonymised or aggregated data unless named data is genuinely needed.

6. Lawful bases, special category and criminal offence data

NILO identifies and records a lawful basis before it starts any new processing. The six lawful bases under Article 6 UK GDPR are consent, contract, legal obligation, vital interests, public task and legitimate interests. As a charity, NILO will not normally rely on public task.

Consent. Where NILO relies on consent, it must be freely given, specific, informed and unambiguous, given by a clear positive action, and as easy to withdraw as to give. NILO keeps records of who consented, when, how and to what. Consent is not used where there is a clear imbalance of power, such as making a grant conditional on it.

Special category data (for example, the health or ethnicity of beneficiaries, or equality monitoring of applicants) needs both an Article 6 basis and an Article 9 condition. NILO will usually rely on explicit consent, employment law obligations, or a substantial public interest condition in Schedule 1 of the Data Protection Act 2018, such as equality of opportunity monitoring or safeguarding of children and individuals at risk.

Criminal offence data (for example, DBS checks or adverse findings uncovered during due diligence) may only be processed under a condition in Schedule 1 of the Data Protection Act 2018, such as preventing or detecting unlawful acts or safeguarding.

Where a Schedule 1 condition requires it, NILO keeps an **Appropriate Policy Document** explaining how it handles that data and how long it keeps it. Equality monitoring data is collected separately from application data and is not seen by assessors or decision-makers.

Children's data. If NILO processes data about children, it takes extra care, uses age-appropriate language, and seeks parental consent for children under 13 for online services and images.