VISION ACTION DATA PROTECTION POLICY *(GLOBAL)*

Co-CEO Foreword

At Vision Action, protecting personal information is essential to maintaining the trust of our beneficiaries, supporters, partners, and colleagues. As an organisation operating across multiple countries, we recognise that safeguarding personal data is a shared global responsibility. We are committed to ensuring that personal data is handled with care, respect, and integrity in every location where we work.

This Data Protection Policy explains how Vision Action complies with the UK General Data Protection Regulation (UK GDPR) and other applicable data protection laws in the countries in which we operate. It sets out our approach to collecting, using, storing, and safeguarding personal data, and how we uphold the rights of individuals across all programmes and offices.

Data protection is fundamental to our organisational values and to protecting the people we serve. It strengthens trust, supports accountability, and reduces risk. We expect all staff, volunteers, trustees, and partners, globally, to follow this policy and seek guidance whenever needed.

Tiwonge Mwase-Vuma

Co-CEO

Jale Canlibalik

Co-CEO

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

Contents

1. Introduction 2

2. Definitions 3

3. Data Protection Principles 3

4. Types of Data We Hold 3

5. Rights of Individuals 4

6. Lawful Bases for Processing 5

7. Images, Videos and stories 5

8. Access to Data (Subject Access Requests) 5

9. Data Disclosures 6

10. Data Security 6

11. Data Protection Impact Assessments (DPIAs) 7

12. Third-party Processing 8

13. International Data Processing and Compliance 8

Country Data Protection Leads 9

14. Data Breaches 9

15. Training 9

16. Records of Processing 9

Data Retention and Disposal 10

17. Complaints 10

18. Data Protection Compliance 10

ANNEX A: DATA PROTECTION POLICY COMPLIANCE 11

ANNEX B: RETENTION PERIODS TABLE 11

ANNEX C: AFRICAN DATA PROTECTION FRAMEWORK (ADPF) 12

Data Protection Documents 14

VISION ACTION DATA PROTECTION POLICY *(GLOBAL)*

1. Introduction

Vision Action applies the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (as amended), together with the Data (Use and Access) Act 2025 where applicable, as its organisational data protection standard. Where personal data is collected, processed or stored in another country, Vision Action also complies with applicable local data protection legislation. Where requirements differ, Vision Action will apply the higher standard of protection unless local law requires otherwise.

Vision Action needs to collect and use information about people with whom we work, including employees, volunteers, trustees, supporters, donors, beneficiaries, partner organisations, contractors, and other individuals connected to our charitable activities. Personal information must

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

always be handled responsibly, securely, and lawfully, whether collected on paper, electronically, or by other means.

We regard the lawful and correct treatment of personal information as fundamental to our work and to maintaining trust and confidence with everyone who engages with us.

This policy applies to all personal data processed by Vision Action in any form and across all activities, including HR, fundraising, programme delivery, supporter engagement, and operations. It applies equally to all employees, volunteers, trustees, supporters, donors, contractors, and beneficiaries (together known as "relevant individuals").

2. Definitions

- **Personal data**: Any information relating to an identifiable person, directly or indirectly (an "identified or identifiable natural person").
- **Special category data**: Data relating to health, racial or ethnic origin, religion or belief, sexual orientation, political opinions, trade union membership, or biometric/genetic identifiers used for identification purposes.
- **Criminal offence data**: Information about criminal convictions or offences and related security measures.
- **Processing**: Any operation performed on personal data, including collection, storage, retrieval, sharing, use, or deletion.

3. Data Protection Principles

Vision Action processes all personal data according to the following principles:

- Data is processed **fairly, lawfully and transparently**.
- Data is collected for **specific, explicit and legitimate purposes**.
- Data is **adequate, relevant and limited** to what is necessary.
- Data is **accurate and kept up to date**.
- Data is retained **only for as long as necessary**.
- Data is processed using appropriate **security and technical measures**.
- Any international transfers comply with **UK GDPR rules on data transfers**.

4. Types of Data We Hold

All data is held only where required for our legitimate charitable purposes.
We hold different types of data depending on our relationship with an individual. This may include:

Employees, Volunteers and Trustees

- Personal contact details and employment/volunteering records
- Payroll, tax and bank information (where relevant)
- Recruitment and vetting data including CVs, references, right to work documentation and records of background checks where required
- Limited criminal offence data relating to DBS or other background checks where lawful and necessary for safeguarding, recruitment or regulatory purposes
- Training, performance and HR records
- Health or medical information where necessary

Supporters, Donors and Members

- Contact details
- Donation history and Gift Aid information

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

- Communication preferences
- Records of interactions and engagement

Programme Beneficiaries and Partners

- Contact details
- Needs assessments and service-related information
- Health and disability information where necessary for programme delivery, patient referrals, monitoring, evaluation, impact measurement, safeguarding, and reporting to donors and funders
- Project related documentation

Vision Action may process special category personal data, including health-related information, received from partner organisations, Ministries of Health, healthcare providers and implementing partners where necessary to support patient referrals, programme delivery, monitoring, evaluation, impact measurement, safeguarding activities and reporting to donors and funders. Such processing will only be undertaken where an appropriate lawful basis and special category condition have been identified and documented, and appropriate safeguards are in place to protect the rights and freedoms of data subjects.

5. Rights of Individuals

Vision Action recognises the rights of individuals under the UK GDPR and, where applicable, relevant data protection legislation in the country where personal data is collected or processed. These rights include:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling

Vision Action implements these rights through the UK GDPR Individual Rights Procedure

All staff must:

• Recognise potential rights requests in any format
• Immediately forward requests to the Information Access Manager (IAM)
• Not respond directly unless authorised

All requests must be logged and managed in accordance with the UK GDPR Individual Rights Procedure.

More information on the rights of individuals can also be found in our privacy notice on our website and at the Information Commissioner's Office website.

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

6. Lawful Bases for Processing

We process personal data only where a lawful basis applies, including:

- Consent (which is specific, informed, freely given, and easily withdrawn)
- Contract
- Legal obligation
- Vital interests
- Public task/legitimate interests (including recognised legitimate interests under the Data (Use and Access) Act 2025 DUAA)

7. Images, Videos and stories

Under lawful basis of consent (which is specific, informed, freely given, and easily withdrawn), we store and process images, videos and stories of beneficiaries which we retain for a maximum period of five (5) years from the date of capture, unless consent is withdrawn earlier.

This period has been determined following an assessment of:

- the purposes for which the images are processed (fundraising, awareness, reporting to donors and stakeholders);
- the expectations of the data subjects at the time consent is obtained;
- the operational scale and resource constraints of the charity;
- the need to evidence impact over multi-year funding cycles; and
- the risk profile of the processing activity.

As a small charity delivering a limited number of projects annually, a five-year retention period ensures we can demonstrate programme impact across long-term grant and funding cycles (often 3–5 years), while avoiding excessive repeat collection of imagery from beneficiaries. It also allows us to build a library of stories that demonstrate the long-term effectiveness of the charity's work.

Images are stored securely and are subject to periodic review. Where images are no longer required, consent is withdrawn, or the retention period expires, they are securely deleted in accordance with data protection and safeguarding requirements.

8. Access to Data (Subject Access Requests)

Individuals have the right to request access to their personal data in accordance with the UK GDPR and any applicable data protection legislation.
Vision Action will carry out reasonable and proportionate searches for relevant data, focusing on systems where such information is most likely to be found. We will respond within statutory timeframes and protect any legally privileged or exempt information.

A Subject Access Request (SAR) is a specific type of individual rights request relating to the right of access. Vision Action manages SARs under its SAR Procedure and all other individual rights under the Individual Rights Procedure

Where permitted by applicable legislation, Vision Action will not normally charge a fee unless the request is manifestly unfounded, excessive, or otherwise permitted by law.

We will need to verify your identity in order to provide personal information, in line with our Data Protection policy.

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

More information can be found on the Information Commissioner's Office website. A SAR can be made by emailing or writing to us at info@visionaction.org.uk or through the Information Commissioner's Office . All staff and volunteers must immediately escalate any request for personal data to the IAM

All Subject Access Requests (SARs) must be handled strictly in accordance with the SAR Procedure

Vision Action will:

- Log all SARs in the central SAR register
- Verify identity before disclosure
- Conduct reasonable and proportionate searches
- Maintain a full audit trail of decisions and disclosures
- No personal data may be released outside this process.

SAR Procedure flowchart:

1. Receive SAR → Staff forwards to IAM/DPO immediately
2. Log SAR → Create case file → Acknowledge requester
3. Verify identity
4. Locate data (UK + international systems)
5. Review & redact → Apply exemptions
6. Prepare response → Securely deliver
7. Notify third parties if required
8. Update register → Close case → File evidence

Operational Management of Data Subject Rights

Vision Action maintains a structured approach to managing requests:

- A central SAR and Rights Request Register is maintained by the IAM
- All requests are assigned a unique reference number
- Case files are stored in Governance folder in Vision Action's secure Sharepoint
- Standard templates must be used for all communications
- Deadlines are tracked and monitored
- Quarterly oversight is conducted by the DPO

Failure to follow this process may lead to compliance risk.

9. Data Disclosures

We may share personal data with third parties only, when necessary, such as:

- Payroll providers or pension administrators
- Providers of employee benefits
- Health and safety or occupational health professionals
- Insurance providers
- HMRC, regulators, or law enforcement (where legally required)
- Programme partners (where needed for delivery)
- DBS umbrella company (subject completes)

All disclosures are proportionate and lawful.

10. Data Security

We protect personal information through a range of security measures:

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

- Hard-copy files stored securely in locked cabinets
- Password protected and encrypted digital systems
- Device level security and screen locking
- Restrictions on removable media and encrypted storage when required
- Prohibition of confidential information being left unsecured
- Regular system backups
- Use of Artificial Intelligence (AI) tools must comply with Vision Action's AI Use Guidelines. Personal, sensitive, confidential or beneficiary information must not be entered into AI systems unless specifically approved and assessed in accordance with organisational procedures.

Breaches of security may lead to disciplinary action where relevant.

11. Data Protection Impact Assessments (DPIAs)

Vision Action must complete a Data Protection Impact Assessment (DPIA) before starting any processing activity that could present a high risk to individuals' privacy rights.

A DPIA is required when, for example:

- Special category data is processed (such as health or disability information).
- A new system, technology, or way of processing personal data is introduced.
- Personal data is collected, shared, or analysed on a large scale.
- Personal data is transferred or processed across multiple countries or jurisdictions.
- Any processing is likely to create a significant risk to the rights and freedoms of individuals.

The DPIA must:

- Identify potential privacy and data protection risks.
- Assess the likelihood and impact of those risks.
- Record the measures that will be taken to reduce or manage the risks.
- Be completed before the processing activity begins.

All DPIAs must be completed using Vision Action's approved DPIA Template, available on SharePoint as part of the Information Governance Framework.

The Information Access Manager (IAM) must review all new DPIAs. Where risks remain high or additional oversight is required, the DPIA must be escalated to the Data Protection Officers (DPOs) for review and approval.

The introduction of new AI tools or AI-enabled processing of personal data may require a Data Protection Impact Assessment (DPIA) and must be reviewed by the IAM before implementation.

Country offices must not begin any processing activity that could create a significant risk to an individual's privacy, rights or freedoms until a DPIA has been completed and reviewed in accordance with Vision Action's procedures.

Examples of high-risk processing include:

- Processing health, disability or other special category data.
- Processing personal data relating to children or vulnerable individuals.
- Using new technologies that process personal data.
- Large-scale collection, monitoring, sharing or analysis of personal data.
- Transferring personal data internationally where additional privacy risks may arise.

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

Any locally developed DPIA processes must align with Vision Action's organisational framework and may be reviewed by the DPOs.

12. Third-party Processing

Where we use third-party processors, we have appropriate contractual arrangements in place to ensure compliance with the UK GDPR and applicable data protection legislation in the jurisdictions in which we operate.

13. International Data Processing and Compliance

Vision Action operates internationally and may transfer or access personal data outside the UK. Some transfers may be necessary due to programme delivery, partnerships, or donor requirements. Vision Action adopts the UK GDPR as its baseline organisational standard for data protection. Where personal data is processed in other jurisdictions, Vision Action also complies with applicable local data protection legislation. Where standards differ, the higher level of protection will normally apply unless local legislation requires a different approach.

All transfers of personal data outside the UK/EEA are limited to what is necessary and are protected through appropriate safeguards, including contractual clauses and secure transfer methods.
Where personal data is processed or accessed internationally:

- Transfers are limited to what is necessary
- Appropriate safeguards are applied
- Local offices must cooperate with SARs and individual rights requests
- Oversight remains with the UK-based IAM and DPOs
- Local practices must align with Vision Action's global data protection framework and not operate in isolation

Personal data, including special category (sensitive) data, collected in the countries in which we operate (including Ghana, Ethiopia, Sierra Leone, and Zambia) may be transferred to and processed in the European Economic Area (EEA), including Germany and Ireland (where our data hosting providers are located), and, where necessary, in the United Kingdom.

We will ensure that all international transfers of personal data are carried out in compliance with applicable data protection laws in the country of origin, as well as relevant UK and EU data protection requirements. Where personal data is transferred across borders, we will implement appropriate safeguards to ensure that it receives an adequate level of protection. These safeguards may include reliance on adequacy decisions, contractual protections such as Standard Contractual Clauses, and appropriate technical and organisational security measures.

We take additional care when transferring special category (sensitive) data to ensure that it is processed securely and only where necessary and lawful.

The Board of Trustees retains overall accountability for data protection across all jurisdictions, with operational management led by the IAM and oversight provided by the DPOs.

No country office may develop or implement data protection policies independently of the organisation's central framework without review and approval by the DPOs. Failure to align local

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

practices with organisational requirements may result in increased regulatory, legal, and reputational risk to the charity.

Country Data Protection Leads

Where required to meet local legal or operational requirements, Vision Action may appoint Country Data Protection Leads in specific jurisdictions. Country Data Protection Leads are responsible for supporting local compliance with applicable data protection laws and ensuring that day-to-day practices align with Vision Action's global data protection framework.

All Country Data Protection Leads must:

- Work in close coordination with the Information Access Manager (IAM)
- Escalate issues, risks, and requests to the IAM and Data Protection Officers (DPOs)
- Follow all organisational policies, procedures, and reporting requirements
- Ensure local practices do not operate independently of the organisation's framework

Country Data Protection Leads do not replace or override the authority of the IAM or DPOs.
The Board of Trustees retains overall accountability for data protection across all jurisdictions. The DPOs (Co-CEOs) are responsible for oversight, and the IAM is responsible for operational management across the organisation.

A separate addendum to this policy '**African Data Protection Framework Addendum**' provides guidelines for country programmes.

14. Data Breaches

All data breaches must be reported internally to both the Compliance Lead and CEO who will immediately escalate it to the Chair of Board.

Vision Action records all breaches and, where legally required, reports them to the ICO within **72 hours** and notifies affected individuals.

15. Training

All employees and volunteers receive training on:

- Confidentiality
- Data protection
- Breach procedures

Training includes mandatory instruction on:

- Recognising Subject Access Requests and individual rights requests
- Escalation to the Information Access Manager
- Use of the SAR and Individual Rights Procedures

Short annual scenario-based refresher training will also be delivered to all staff. (Example: "Someone emails asking for their records — what do you do?")

Completion of training is recorded and monitored using the organisation's BrightHR platform. Those with specialist responsibilities receive additional training.

16. Records of Processing

Vision Action maintains up-to-date records of all processing activities, including purposes and retention periods. The Record of Processing Activities (ROPA) is maintained by the Compliance Lead

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

and stored on Vision Action's secure Sharepoint and is reviewed annually.

Data Retention and Disposal

Vision Action retains personal data only for as long as necessary to fulfil its legitimate purposes and to meet legal, regulatory, and contractual obligations.

Retention periods are defined in the organisation's Data Retention Schedule (ANNEX B) and apply across all country offices.

All personal data must be:

- Reviewed periodically to ensure it is still required
- Stored securely throughout the retention period
- Deleted or destroyed securely when no longer needed

Secure disposal methods include:

- Shredding of physical documents
    - DIN P-4 compliant cross-cut shredders and the output inspected for no remaining identifiable text
- Permanent deletion of electronic data
- Secure wiping or destruction of storage devices

Country offices must align with Vision Action's retention framework and must not apply retention periods independently without approval from the IAM and DPOs.

17. Complaints

In accordance with the **Data (Use and Access) Act 2025** (DUAA), Vision Action operates an internal **data protection complaint handling process**. We will:

- Acknowledge complaints within **30 days**
- Investigate without undue delay
- Keep individuals informed
- Provide an outcome in writing

Individuals retain the right to contact the UK Information Commissioner's Office (ICO). Where personal data is processed in another jurisdiction, individuals may also have rights to complain to the relevant supervisory authority in that country.

18. Data Protection Compliance

For the purposes of this policy, Judith Trigg, Grants and Organisational Compliance Lead (judith.trigg@visionaction.org.uk), acts as the Information Access Officer and is responsible for day-to-day data protection matters.

Tiwonge Mwase-Vuma and Jale Canlibalik, Co-CEOs (Tiwonge.Mwase-Vuma@visionaction.org.uk; Jale.Canlibalik@visionaction.org.uk), act as the Data Protection Compliance Officers and are responsible for oversight, significant compliance decisions and escalations.

Vision Action will monitor compliance with this policy through periodic reviews of data protection practices, retention records, data breach reports, training completion records, and records of processing activities. Any identified gaps or risks will be addressed through corrective actions, additional training, process improvements, or updates to documentation where required.

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

ANNEX A: DATA PROTECTION POLICY COMPLIANCE

I have received and been briefed on the Vision Action Data Protection Policy and its training papers and fully understand my responsibilities to comply with and promote the Policy.

Signed	
Name	
Position within Vision Action	
Date	

ANNEX B: RETENTION PERIODS TABLE

Data Type	Example	Retention	Reason
HR records	Staff files,	6 years post-employment	Legal claims limitation period; employment law compliance
Financial	Accounts, invoices	6–7 years	Statutory accounting, tax and audit requirements
Consent	Membership, event sign up, donors and donations, marketing, volunteering	24 months or until 24 months after the last donation	Legitimate organisational relationship management; consent records retention; Aligns to Privacy Policy
Programme/ M&E	Surveys, beneficiary data	3–5 years post project	Funder, reporting and audit requirements
Images/media	Photos/videos	5 years	Consent management and organisational communications
Contracts	Supplier agreements	6 years post-end	Contractual obligations and limitation period for legal claims
Legacies	Will legacies	Ongoing, lifetime commitment due to the long-term nature of legacy administration. Then 6 years post estate settlement	Administration of estates, legal obligations and donor stewardship; aligns to Privacy Policy

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

ANNEX C: AFRICAN DATA PROTECTION FRAMEWORK (ADPF)

Organisation-Wide Standard for All Africa Programmes

1. Purpose and Scope

This framework sets the organisation's minimum data protection standard across all African programmes. It ensures lawful processing, protection of sensitive (including children's health) data, consistent cross-border governance, and clear accountability.

Applies to all African country programmes and all personal data processed.

Aligned with UK GDPR, EU GDPR principles, and applicable local laws and data protection principles.

2. Core Principle

A single GDPR-equivalent standard applies across all programmes, supplemented by country addendums. Where local law is stricter, it prevails.

3. Data Protection Principles (Global Standard)

All programmes must comply with:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

4. Data Roles and Governance Model

The organisation operates a multi-controller model.

- Controllers (e.g. UK office, ministries, implementing partners) determine purpose, use, and sharing.
- Processors (e.g. Toladata – Germany, Microsoft SharePoint – UK) act only on documented instructions and do not determine purpose.

5. Children's Health Data Standard

Children's eye health data is treated as highly sensitive.

- Data should be anonymised or aggregated where possible.

Identifiable data requires:

- a lawful basis
- valid consent or legal justification
- enhanced safeguards

6. International Data Transfers

All cross-border transfers must comply with applicable data protection laws and ensure an adequate level of protection.

Transfers must:

- use a lawful transfer mechanism

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

- be approved and documented
- be limited to necessary data and purposes
- apply appropriate technical and organisational safeguards
- use approved jurisdictions or systems (e.g. EEA/UK)

Additional safeguards are required for sensitive data.

7. External Data Sharing (Including donors and research)

All external sharing (donors, research, third parties) requires:

- formal assessment
- Data Sharing Agreement
- ethics approval (or exemption) where applicable

Must ensure:

- no re-identification
- no onward sharing
- secure institutional storage
- defined retention and deletion

8. Minimum Security Standard

Applies to all countries:

- no storage on personal devices
- access restricted to authorised users
- encrypted transfer where possible
- secure institutional systems only
- audit trail required where systems allow

9. Accountability

- Compliance Lead and Co-CEOs: cross-border governance and approvals
- Global MEAL Lead: local compliance and implementation oversight
- Country Directors: risk acceptance
- Data Processor: technical security only

10. Relationship to Country Addendums

This framework is **superseded only by stricter local law**, implemented via country addendums.

COUNTRY ADDENDUMS

All countries:

- Registration requirements with Data Protection Commission apply where relevant
- Registered Data Protection Leads if applicable
- Parental/guardian consent required for children's data
- Local implementing partners may act as (joint) controllers
- Cross-border transfers must comply with applicable law and require appropriate safeguards
- Research requires ethics approval and Data Sharing Agreement
- Global MEAL Lead must confirm local consent and implementation

In addition, the following country-specific requirements apply:

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)

Ghana Addendum

- Governed by **Data Protection Act 2012**
- Cross-border transfers (Ghana → EU/UK) require safeguards and approval
- External sharing requires joint Ghana + UK approval

Zambia Addendum

- Governed by **Zambia Data Protection Act 2021**
- Cross-border transfer (Zambia → EU/UK) requires documented safeguards and controller approval
- External sharing requires joint Zambia + UK approval

Sierra Leone Addendum

- Governed by **Data Protection Act 2022**
- Regulatory enforcement is developing but law applies fully
- Cross-border transfers (Sierra Leone → EU/UK) require enhanced safeguards and documented approval
- Strict oversight for external data sharing due to evolving regulatory environment

Ethiopia Addendum

- No comprehensive GDPR-equivalent law currently in force
- The organisation applies a UK GDPR-equivalent internal standard
- Relevant Ethiopian laws on privacy and cybercrime apply
- Vision Action UK acts as primary controller by default (unless otherwise defined)
- External sharing is highly restricted (prefer anonymised or aggregated data) and requires UK approval
- Identifiable data export requires Vision Actions UK Data Protection Officer (CO-CEOs) approval
- Research sharing requires ethics approval, Federal Ministry of Health approval, and a Data Sharing Agreement

Data Protection Documents

Code	Name	Document type	Where to find it
DP01	Data Protection Policy (Global)	Policy	This document
DP02	Individual Rights Procedure	Procedure	Sharepoint, HR & Admin
DP03	SAR Procedure	Procedure	Sharepoint, HR & Admin
DP04	SAR Templates	Templates	Sharepoint, HR & Admin
DP05	DPIA Template	Template	Sharepoint, HR & Admin
DP06	Retention Schedule	Schedule	ANNEX B of this document
DP07	African Data Protection Framework (ADPF)	Framework	ANNEX C of this document
DP08	Data Protection Awareness Brief	Training	Sharepoint, HR & Admin
DP09	Data Protection Essentials Guidance	Guidance	Sharepoint, HR & Admin
IT02	AI Use Guidelines	Guidance	Sharepoint, HR & Admin
PN01	Public Privacy Notice	Notice	Sharepoint, HR & Admin
PN02	Employee Privacy Notice	Notice	Sharepoint, HR & Admin

Vision Action – Registered Charity No. 1081695 (England & Wales)
Companies House registration No. 4027804 (England & Wales)