

ACCOUNTABILITY LAB GLOBAL

Document 19: Information, Data and Digital Security Policy

Document number	19 of 20
Status	Approved
Owner	Co-CEO, Innovation and Operations, with the Director of Finance for asset management
Approved by	AL Global Board of Directors, on the recommendation of the Governance Committee
Date adopted	<i>24 September 2026</i>
Adopted by	<i>AL Board of Directors</i>
Effective from	<i>24 September 2026</i>
Review cycle	Annually
Next review due	<i>24 September 2027</i>
Part of	The AL Global policy set, Documents 00 to 20. Document 00, the Alignment, Roles and Ownership Register, is the control document for the set.

ACCOUNTABILITY LAB GLOBAL.....	1
Document 19: Information, Data and Digital Security Policy.....	1
1. The risk this policy is actually about.....	2
2. Scope.....	3
3. Information classification.....	3
4. Protecting people, not just data.....	4
4.1 Minimise.....	4
4.2 Consent that means something.....	4
4.3 Hostile environments.....	5
4.4 When it goes wrong.....	5
5. Data protection compliance.....	5
5.1 Standard.....	5
5.2 Principles.....	5
5.3 What AL must maintain.....	5
5.4 Individual rights.....	6
5.5 Ownership.....	6
6. Digital security.....	6
6.1 Everyone.....	6
6.2 AL.....	6
6.3 Incident response.....	7
7. Devices, equipment and disposal.....	7
8. AI tools.....	8
9. Social media and public communications.....	8
9.1 Speaking for AL.....	8
9.2 Speaking for yourself.....	8
9.3 A caution AL should give its own people.....	9
10. Retention.....	9
11. Oversight.....	9

Relationship to the AL Network AI Policy. AL has a separate Network AI Policy effective 1 June 2026. **This policy does not amend it and does not restate it.** Where the two touch, the AI Policy governs the use of AI tools and this policy governs the underlying handling of information. Section 8 sets out how they fit together.

1. The risk this policy is actually about

Most information security policies are written around commercial confidentiality: pricing, customer lists, intellectual property. AL's risk is different in kind.

AL holds information that can get people arrested, dismissed from their jobs, driven from their homes, or killed. The names of whistleblowers who reported corruption in their own institutions. The identities of community monitors and citizen reporters in countries where that work is treated as subversion. Testimony from survivors of abuse. Locations, movements and associations of staff and partners in hostile environments.

This policy is built around the proposition that for AL, an information breach is a safeguarding failure before it is a compliance failure. That is why “endangerment through disclosure” is listed as a form of harm in the Safeguarding and PSEAH Policy, and why serious breaches escalate to the Global Safeguarding Lead as well as through the technical route.

2. Scope

Tier 1, directly and in full. AL Global employees, **including employees of Model A fiscally sponsored projects**, board members, fellows, interns, volunteers, consultants and contractors while engaged on AL work. Applies to all AL information wherever held: AL systems, personal devices used for AL work, cloud services, paper, and anything in someone’s head that they might say out loud in the wrong place.

Tier 2, by agreement. Model C fiscally sponsored clients, sub-awardees, grantees and suppliers handling AL information, through their agreements. Equivalence assessed and recorded by the Co-CEO, Innovation and Operations at onboarding and reviewed annually.

Tier 3, by collective adoption. Network Labs are autonomous. AL Global proposes network-wide information standards through the Network Council. **Governance Compact section 9.3 already provides that where data protection standards differ between Labs, the higher or more protective standard prevails**, which is a sound principle and a foundation to build a network standard on.

3. Information classification

Four levels. Everyone should be able to say which level a document is at.

Level	What it covers	Handling
Protected	Anything that could expose a person to harm: identities of whistleblowers, community monitors, citizen reporters and survivors; safeguarding records; security incident details; sources for investigative work; location data for staff in hostile environments	Named individuals only, on a need-to-know basis recorded by the owner. Encrypted at rest and in transit. Never on personal devices, personal accounts, or unencrypted messaging. Never discussed in public places or on calls in shared spaces. Minimum retention
Confidential	Personnel records, pay, health information, donor agreements, financial records, legal advice,	Role-based access. Encrypted. Not shared outside AL without authorisation

Level	What it covers	Handling
	board papers, unpublished research	
Internal	Ordinary working documents, plans, drafts, internal communications	Available across AL. Not published
Public	Published reports, website content, approved communications	No restriction

When in doubt, treat information as one level higher. The cost of over-protecting a document is inconvenience. The cost of under-protecting a Protected one can be someone's liberty.

4. Protecting people, not just data

This section takes precedence over everything else in this policy.

4.1 Minimise

Do not collect what you do not need. The safest data is data AL never held. Before collecting names, contact details, photographs, locations or testimony, ask what AL actually needs and for how long.

Where possible, use pseudonyms, reference codes or aggregated data. Keep the key linking a code to a real identity separately, with access restricted to the smallest possible number of named people.

4.2 Consent that means something

Before recording, photographing, quoting, publishing or naming anyone:

- Explain honestly what AL will do with it, who will see it, and **what could go wrong**, including reprisal risk from any political content
- Get consent in a language the person understands
- Make clear that refusing costs them nothing
- Record the consent, and record what it covered

Consent to be interviewed is not consent to be named. Consent to be named in a report is not consent to appear in a social media post. Ask separately.

Consent can be withdrawn. Where someone asks to be removed, AL removes what it can and tells them honestly what it cannot remove and why.

4.3 Hostile environments

- **Assume devices may be seized** at borders, checkpoints or during a search. Travel with clean devices where the risk warrants it. See the Duty of Care, Safety and Security Policy for pre-travel preparation.
- **Assume communications may be monitored.** Use end-to-end encrypted channels for anything Protected. Do not use SMS or unencrypted email for identities.
- **Have a plan for compelled disclosure.** Where someone may be forced to unlock a device, the answer is that the device should not contain Protected information in the first place.
- **Publishing decisions involving identifiable people in hostile environments** require sign-off from the relevant Country Director or project lead and, where anyone is at risk, the Global Safeguarding Lead.

4.4 When it goes wrong

Any breach involving Protected information is escalated immediately to the Co-CEO, Innovation and Operations and to the Global Safeguarding Lead, in parallel, not in sequence.

The first question is not “what is our regulatory exposure”. It is “**who is now at risk, and what do we do about it today**”. Warning the affected person, moving them, funding relocation or legal support through the Safety and Security Fund all come before any notification process.

5. Data protection compliance

5.1 Standard

AL applies GDPR as its global floor, because it travels better than the US state-by-state patchwork and because much of AL’s network sits in or works with jurisdictions that expect it. Where a country’s law is stricter, that law applies.

This mirrors Governance Compact section 9.3.

5.2 Principles

Personal data must be processed lawfully and fairly; collected for specified purposes and not used incompatibly; adequate, relevant and limited to what is necessary; accurate and kept up to date; kept no longer than necessary; and kept secure.

5.3 What AL must maintain

- **A record of processing activities**, replacing the “Register of Systems” the old policy promised. Owned by the Co-CEO, Innovation and Operations. Reviewed annually. **If this does not currently exist, it is a live audit finding and building it is the first task under this policy.**

- **Data protection impact assessments** for high-risk processing. For AL this means any programme involving identifiable community monitors, citizen reporters or survivors, particularly in hostile environments.
- **Data processing agreements** with every supplier that handles personal data on AL's behalf.
- **Privacy notices** for staff, participants and website users.
- **A breach log**, with dates, what happened, who was affected, what was done, and what changed.

5.4 Individual rights

People whose data AL holds may request access, correction, deletion, restriction, portability, and may object to processing. Requests go to the Co-CEO, Innovation and Operations and are answered within one month.

Verify identity carefully before disclosing anything, and where the request touches Protected information, involve the Global Safeguarding Lead.

5.5 Ownership

Data protection compliance sits with the **Co-CEO, programs and Learning**. Day-to-day administration may be delegated, accountability may not.

6. Digital security

6.1 Everyone

- Unique, strong passwords, managed in an approved password manager. No reuse, no sharing.
- **Multi-factor authentication on every account that supports it.** This is the single highest-value control AL has.
- Devices locked when unattended, encrypted at rest, with automatic screen lock.
- Updates and patches applied promptly.
- Approved AL systems for AL work. Personal email and personal cloud accounts are not used for AL information.
- Report anything suspicious immediately. **Reporting a suspected phishing click is never punished.** People who fear blame do not report, and the delay is what causes the damage.

6.2 AL

- Access granted on the least-privilege principle and reviewed at least annually.
- Access revoked on the last working day, in full, including third-party services.

- Backups maintained and, at least annually, **tested by restoring from them**. An untested backup is a hope.
- Endpoint protection on AL devices.
- Logging and monitoring proportionate to the risk, and transparent to staff.
- Phishing awareness training at induction and annually.
- Supplier security assessed before any service handling Confidential or Protected information is adopted.

6.3 Incident response

- **Contain.** Disconnect, revoke access, change credentials.
- **Escalate immediately** to the Co-CEO, Programs and Learning. Where Protected information is involved, to the Global Safeguarding Lead in parallel.
- **Assess who is at risk** and act on that first.
- **Assess notification duties:** data protection regulators, donors under grant terms, and **2 CFR 200.113 mandatory disclosure** where a federal award is affected and the incident involves fraud.
- **Record** in the breach log.
- **Fix the cause** and track the fix to completion.

7. Devices, equipment and disposal

This section replaces the Laptop Asset Disposal Policy.

- AL maintains an asset register of all devices, with holder, serial number and encryption status. Owned by the Director of Finance.
- Devices are encrypted before issue.
- On return, devices are **securely wiped to a standard that prevents recovery** before reuse, donation, sale or disposal. Wiping is recorded against the asset register entry.
- **A device that held Protected information is wiped by AL and never passed on unwiped**, including to another staff member.
- Physically destroyed drives are certified as destroyed.
- Lost or stolen devices are reported the same day and treated as a security incident under section 6.3.
- Paper records are shredded, not binned.

Equipment disposal on a federal award may be subject to 2 CFR 200.313 property standards, including disposition requirements above a threshold. The Director of Finance should confirm the position with your auditor before disposing of federally funded equipment.

8. AI tools

AL has a separate Network AI Policy, effective 1 June 2026, which governs the use of AI tools. This policy does not amend it, restate it or override it.

Where the two meet, the division is:

- **The AI Policy governs** which tools may be used, for what, with what approvals and oversight, and the roles that manage that.
- **This policy governs the information** that goes into those tools. In particular: **Protected information is never entered into any AI tool**, whatever the AI Policy permits for other categories, and the classification in section 3 applies to AI inputs exactly as it applies to email, documents and messaging.

Anyone using AI tools at AL should read both.

9. Social media and public communications

This section replaces the Social Media Policy and the social media provisions of the Employee Handbook.

9.1 Speaking for AL

Only people authorised by the Co-CEOs post on AL's official channels. Content follows the same information classification and consent rules as anything else AL publishes.

9.2 Speaking for yourself

Staff are entitled to their own social media presence and their own opinions. AL does not monitor personal accounts and does not require staff to represent AL in their private lives.

What is required:

- Be clear when you are speaking personally rather than for AL.
- **Never post Protected or Confidential information**, including photographs that could identify a monitor, participant or colleague, or that reveal a location.
- Do not post anything that harasses, demeans or discriminates. The Code of Conduct applies online.
- Do not post about a live investigation, safeguarding matter or security incident.

- Think about who else your post exposes. A photograph of a workshop can identify every person in it.

9.3 A caution AL should give its own people

For staff in several countries where AL works, a personal social media post can attract state attention to the individual and to their colleagues. **AL will not discipline anyone for their lawful personal political expression**, and AL will support anyone who faces consequences for it. But managers should make sure people, particularly younger staff and fellows, understand the risk in their own context rather than assuming they do.

10. Retention

Information is kept only as long as it is needed, then securely destroyed.

AL does not currently have a document retention policy and needs one. Until it does:

- Federally funded records follow **2 CFR 200.334**, generally three years from submission of the final financial report, with exceptions. Confirm the applicable period with your auditor.
- The fiscal sponsorship agreement with Accountable Now sets **seven years** following termination, or the funder's period if longer.
- **Safeguarding records are retained longer than standard personnel records**, because historic disclosure is common in this field. The exact period needs legal input per jurisdiction and I have deliberately not put a number on it.
- **Protected information is retained for the shortest period that serves the purpose**, and the default is deletion.

11. Oversight

- The Co-CEO, Programs and Learning reports at least twice yearly to the Governance Committee on incidents and near misses, the record of processing activities, access review completion, backup restore testing, training completion, and outstanding actions.
- Serious incidents go to the Board.
- **Near misses are reported and welcomed.** They are the cheapest warning AL will get.
- This policy is reviewed annually.