

GAIA
Internet-Draft
Intended status: Informational
Expires: 15 September 2026

L. Navarro
ISOC.CAT
M. Roura
eReuse.org
E. Rodriguez
TAU/RAEE
V. Ambrosi
EKOA, Facultad de Informática - UNLP
14 March 2026

Operational Practices for Digital Sovereignty and Meaningful
Connectivity through Circular Management of User and Network Devices
draft-gaia-circular-device-practices-01

Abstract

This document systematizes operational practices observed across multiple community-centred deployments that aim to improve meaningful connectivity and digital sovereignty through the circular management of end-user and network devices. It is published as an Informational RFC on the IRTF stream and does not define Internet standards or protocol requirements.

The document addresses a foundational but often overlooked dependency of Internet connectivity deployments: the availability, repairability, governance, and lifecycle management of network and end-user devices required for meaningful participation in the Internet. Based on operational experience from deployments in Spain, Argentina, and Senegal including eReuse.org, EKOA/UNLP, SolidanTera, TAU/RAEE, and Hahatay this document describes practices that have demonstrated positive outcomes for connectivity, social inclusion and community capacity, and environmental sustainability.

These practices are presented as descriptive guidance derived from operational experience rather than as normative requirements. They complement research within the IRTF GAIA Research Group by documenting reproducible approaches that improve the sustainability, autonomy, and long-term viability of Internet access in underserved contexts.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 15 September 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction	3
1.1. Background and Relationship to Prior IRTF Work	5
1.2. Meaningful Connectivity: Context and Frameworks	5
1.3. Relevance to IRTF GAIA	6
2. Terminology and Scope	6
3. Problem Statement	9
4. Principles Derived from Operational Experience	10
4.1. Device Availability as a Foundational Layer of Connectivity	10
4.2. Local Capacity, Repairability, and Digital Sovereignty .	10
4.3. Collective Access Models and Commons-oriented Governance	11
4.4. Transparency, Traceability, and Trust across the Lifecycle	11
4.5. Repairability and Lifecycle Extension as Environmental and Social Strategy	12
4.6. Privacy and Security Embedded in Reuse Workflows	12
4.7. Environmental Responsibility across the Full Device Lifecycle	12
4.8. Community-rooted Governance and Social Relevance	13
5. Operational Practices	13
5.1. Digitalised Circular Device Management	13
5.2. Repair, Training, and Capacity Building	14

5.3.	Alignment with Connectivity Infrastructure	14
5.4.	Community-centred Meaningful Connectivity	15
5.5.	Collective Access and Commons-based Device Governance . .	15
5.6.	Federated Registries and Cross-community Coordination . .	16
5.7.	Secure Data Sanitisation	16
5.8.	Architectural Considerations for Connectivity Infrastructure	17
6.	Human Rights, Security, Privacy, and Sustainability Considerations	17
6.1.	Human Rights	17
6.2.	Security	18
6.3.	Privacy	19
6.4.	Environmental and Sustainability	20
7.	Deployment Case Studies (Informative)	20
7.1.	Catalonia and Madrid (Spain): eReuse.org ecosystem and social enterprises	20
7.2.	La Plata (Argentina): EKO/UNLP programmes integrating refurbishment, training, and outreach	21
7.3.	Hahatay (Senegal): Device availability and inclusion in rural and peri-urban contexts	22
7.4.	Rosario (Argentina): TAU/RAEE and territorial programmes in villas	23
8.	Replication Guidelines	24
9.	Implications for Research and Deployment	24
10.	IANA considerations	25
11.	Acknowledgements	25
12.	References	25
12.1.	Informative References	25
12.2.	Informative References	25
	Authors' Addresses	27

1. Introduction

Extending Internet connectivity requires more than deploying network infrastructure. Meaningful participation in the Internet also depends on the availability of functional, affordable, and maintainable devices, including end-user devices (e.g., laptops and phones) and, in many deployments, networking equipment such as routers, switches, and antennas. In underserved communities, limited device availability is often a primary barrier to benefiting from existing or planned connectivity.

While electronic devices cannot be fully circular in a strict material sense, circular device management refers to practices that extend device lifetimes and maximise reuse before final recycling or disposal.

Circular device management encompassing local reuse, repair, refurbishment, redistribution, and responsible end-of-life handling has emerged as an effective approach to address this barrier. Device availability and lifecycle management therefore become architectural considerations for connectivity deployments, rather than purely logistical or procurement concerns. When combined with community-centred governance and digital device management, these practices can improve connectivity outcomes, strengthen local capacity, and reduce environmental impact.

These practices also contribute to digital sovereignty by enabling communities and organisations to exercise greater agency and choice over the technologies and infrastructure they rely on. By strengthening local repair and refurbishment capacity and enabling collective governance of device lifecycles, circular device management reduces dependence on external actors and increases communities' ability to manage and adapt their digital infrastructure according to local needs.

This document draws on operational experience from several deployments, including:

- * eReuse.org deployments in Catalonia and Madrid (Spain), involving social enterprises and reuse circuits that coordinate donors, refurbishers, and recipient organisations;
- * University-linked programmes in Argentina (EKOA/UNLP), integrating refurbishment, training, and community engagement;
- * TAU/RAEE in Rosario (Argentina), where a specialised cooperative carries out device diagnostics, repair, data sanitisation, refurbishment, and e-waste management, while community centres focus on access, accompaniment, and territorial programmes;
- * Hahatay initiative in Senegal, combining device availability with local digital inclusion efforts in rural and peri-urban contexts.

Several initiatives apply collective access and community-ownership models in which devices are managed as shared resources rather than permanently transferred private property [Ostrom1990]. Digital lifecycle tracking supports transparency, accountability, and coordination across donors, refurbishers, and communities, an approach analysed in prior research [Roura2025].

1.1. Background and Relationship to Prior IRTF Work

This document builds on prior IRTF work that recognizes Internet connectivity infrastructure as a socio-technical system in which protocols, infrastructure, governance, and human practices interact. In particular, [RFC8280] established the importance of systematically considering human rights impacts during protocol development, while [RFC9620] further refined practical guidance for identifying and documenting such impacts in IETF and IRTF work.

While this document does not define or modify Internet protocols, it addresses operational dependencies that directly affect whether Internet access architectures can be used in ways that respect human rights, support sustainability, and enable meaningful participation. Device availability, repairability, governance, and lifecycle management shape who can participate in networked systems, under what conditions, and with what degree of autonomy. As such, these operational practices constitute a pre-condition for realizing the rights-aware Internet architectures envisioned in prior IRTF research.

This document therefore complements protocol-level human rights considerations by documenting empirical, deployment-level practices that enable human-centred outcomes in real-world access contexts.

1.2. Meaningful Connectivity: Context and Frameworks

The ITU Universal Meaningful Connectivity (UMC) framework [ITU-UMC] provides a widely recognised baseline by identifying six dimensions of meaningful connectivity: quality, availability, affordability, security, device access, and skills.

Civil-society analyses, notably by APC and the Global Information Society Watch [GISW2024], extend this framing by considering not only technical access (infrastructure, connectivity, devices), but also social relevance, community agency, cultural and political meaningfulness, inclusive governance, and sustainable local ownership. These perspectives recognise that connectivity gains value when aligned with community practices, needs, and aspirations.

The Internet Governance Forum Policy Network on Meaningful Access (PNMA) further emphasises that meaningful connectivity involves the ability of communities to create, publish, and access services and content locally, including in local languages, rather than acting solely as consumers of externally hosted services [IGF-PNMA2024].

Some literature refers to similar concepts using the term “meaningful access”, particularly in civil-society and Internet governance discussions. In this document, the term “meaningful connectivity” is used as the primary label while incorporating these broader perspectives on participation, local services, and community agency.

The definition below, and practices described in this document, adopt this community-centred interpretation of meaningful connectivity.

1.3. Relevance to IRTF GAIA

The IRTF GAIA Research Group investigates technical and socio-technical approaches to extend Internet access to underserved populations. Device availability, repairability, and lifecycle governance form a foundational layer of access architectures and directly affect sustainability, resilience, and adoption. These aspects align with the GAIA research group’s interest in architectures and operational practices that enable local infrastructure, services, and community participation in the Internet ecosystem.

This document is intended to inform GAIA research discussions, architectural exploration, and capacity-building efforts, while showing areas where further research may be valuable. It does not define protocol requirements and does not mandate compliance.

2. Terminology and Scope

This document is published as an Informational RFC on the IRTF stream. It does not specify Internet standards, protocol requirements, or compliance criteria.

Terms such as “should”, “can”, or “may” are used in their ordinary, descriptive sense to convey observed practices and lessons derived from operational experience. They indicate patterns that have been found effective in specific contexts, rather than mandatory or normative requirements.

***Circular device management*:** Structured processes that enable reuse, repair, refurbishment, redistribution, tracking, and responsible recycling of devices.

In this document, the term “circular device management” refers to operational practices that extend device lifecycles through reuse, repair, refurbishment, redistribution, and responsible end-of-life handling.

***Chain of custody*:** A documented record of the sequence of organisations or individuals responsible for a device during its lifecycle, particularly during transfer, refurbishment, allocation, and end-of-life processes, enabling accountability, traceability, and verification of handling and processing steps.

***Collective access/community ownership*:** A governance model in which devices are managed as shared resources, with rights of use, maintenance, and reassignment defined collectively rather than through permanent individual ownership, following a common-pool resource governance model. [Ostrom1990]

***Community-centred infrastructure*:** Digital infrastructure (devices, facilities, local organisations, and governance) that is locally operated and aligned with community needs.

***Commodatum (loan for use)*:** A form of loan [COMMODATE] in which a device is provided to an individual or organisation *for use without transfer of ownership*, typically for a defined or renewable period, and with the obligation to return the device or allow reassignment when the agreed conditions end.

In circular device management contexts, devices provided under commodatum support collective access by enabling maintenance, replacement, traceability, and reassignment of devices over time, while preserving shared stewardship and accountability.

***Device*:** Any Internet-capable end-user or networking device, including laptops, desktops, tablets, smartphones, routers, switches, antennas, access points, and IoT equipment.

***Device commons*:** A community governance model in which devices are managed as shared resources rather than exclusively owned assets, following principles of common-pool resource governance [Ostrom1990].

***Device lifecycle tracking*:** The structured recording of events throughout the operational life of a device, including acquisition, diagnostics, refurbishment, allocation, maintenance, reallocation, and end-of-life handling.

Lifecycle tracking enables accountability, transparency, and coordination across multiple organisations involved in reuse management.

***Device reuse ecosystem*:** A network of organisations and actors involved in device donation, diagnostics, refurbishment, redistribution, and recycling, typically including donors, refurbishers, community organisations, and recyclers.

***Digital sovereignty*:** The ability of individuals, communities, and organisations to exercise meaningful control over the technologies, infrastructure, data, and services that shape their digital environment.

In the context of Internet connectivity and community-centred infrastructure, digital sovereignty includes the capacity to deploy, maintain, repair, govern, and adapt devices, networks, and services locally, while reducing unnecessary dependence on external actors or proprietary constraints. In circular device management contexts, digital sovereignty is strengthened through practices that support device repair and reuse, promote open and interoperable software systems, enable lifecycle transparency, and allow communities and organisations to manage device availability according to their own needs and governance arrangements.

***Federated inventory/registry*:** A network of interoperable device registries that enables transparency, accountability, cross-organisational coordination, and scaling without requiring centralisation.

***Meaningful connectivity*:** Internet access that is available, affordable, reliable, and usable in ways that enable meaningful participation in society and improve people's lives. Achieving meaningful connectivity requires enabling conditions including access to appropriate devices, adequate quality of service, digital skills, security and privacy protections, and the ability of communities to create, publish, and access locally relevant services and content. It also encompasses social relevance, community agency, cultural and political meaningfulness, inclusive governance, and sustainable local ownership.

This interpretation draws on the ITU Universal Meaningful Connectivity framework [ITU-UMC], the Internet Society perspective on meaningful connectivity [ISOC-MC2025], civil-society analyses such as [GISW2024], and work of the Internet Governance Forum Policy Network on Meaningful Access [IGF-PNMA2024].

***Refurbisher*:** An organisation or facility responsible for evaluating, repairing, sanitizing, and preparing devices for reuse.

***Refunctionalisation*:** Refurbishment or remanufacturing processes that return an ICT device to a functional state for continued use, possibly in a different operational or social context.

This definition is aligned with ITU-T L.1081 [ITU-T-L1081].

***Traceability*:** The ability to record, verify and account details about the lifecycle history of a device through digitally recorded events, identifiers, and documentation to enable accountability, impact measurement, and ecosystem coordination.

This document focuses on community/local-scale, decentralised practices relevant to connectivity infrastructure, community/local facilities, and underserved contexts. The practices are described to inform analysis and deployment, not to mandate implementation or establish compliance requirements.

3. Problem Statement

Despite investments in access networks, many communities remain excluded from meaningful connectivity due to:

- * Insufficient availability of functional end-user and network devices for households, schools, and community organisations;
- * Markets dominated by non-repairable or locked-down hardware and software preventing device reuse, with short usage cycles followed by replacement;
- * Limited local repair capacity, including insufficient skills, limited access to spare parts, and limited tools for diagnostics, secure data handling and refurbishment;
- * Lack of interoperable systems to manage and track device lifecycle and accountability across donors, refurbishers, and recipient organisations and persons;
- * Premature disposal of devices, contributing to environmental harm and e-waste;
- * Organisational and ownership models based on permanent individual assignment of devices, which can hinder redistribution, maintenance, reassignment to evolving needs, and scalability;
- * Lack of digitalised device management and transparency tools limits trust among donors and refurbishers, obstructs environmental and social impact assessment, and prevents coordinated processing of large-volume donations.
- * Network connectivity alone cannot solve digital exclusion if individuals lack adequate end-user and networking devices.

Operational experience shows that without collective device access models and digital traceability, communities struggle to pool devices, scale refurbishment, assess impact, or establish donor trust and accountability [Roura2025]. As a result, access networks alone are insufficient to close the digital divide.

Addressing device availability is therefore a foundational requirement for equitable, inclusive, and rights-preserving Internet access.

4. Principles Derived from Operational Experience

This section synthesizes recurring patterns observed across multiple community-centred deployments involving circular device management and access provision. These principles do not constitute prescriptive requirements or normative rules. Rather, they articulate conditions, trade-offs, and enabling factors that have consistently influenced the sustainability, autonomy, and social relevance of connectivity initiatives in practice.

The principles are interdependent and should be interpreted holistically, as they mutually reinforce (or undermine) one another depending on local context, governance arrangements, and resource constraints.

4.1. Device Availability as a Foundational Layer of Connectivity

Operational experience consistently shows that device availability functions as a foundational layer of connectivity, rather than as a peripheral or downstream concern. Even where connectivity infrastructure exists, the absence of adequate end-user or network devices significantly constrains effective use, adoption, and long-term impact.

In practice, connectivity initiatives that explicitly plan for device availability—across initial deployment, maintenance, replacement, and reassignment—are better able to sustain connectivity over time and adapt to changing community needs. Treating devices as part of the connectivity system, rather than as a one-off input, reduces the risk of stranded infrastructure and uneven access outcomes.

4.2. Local Capacity, Repairability, and Digital Sovereignty

Across deployments, local capacity to diagnose, repair, reconfigure, and manage devices has emerged as a critical determinant of sustainability. Dependence on external vendors, proprietary restrictions, or non-repairable hardware often introduces long-term fragility, cost escalation, and loss of local agency.

Operationally, initiatives that invest in repair skills, access to spare parts, and locally understandable software stacks are better positioned to maintain continuity of service and adapt technologies to local conditions. These practices contribute directly to digital sovereignty by enabling communities to exercise meaningful control over the material and technical components of their connectivity.

4.3. Collective Access Models and Commons-oriented Governance

In many underserved contexts, individual private ownership of devices has proven insufficient to address issues of scarcity, affordability, and unequal access. By contrast, collective access arrangements, where devices are treated as shared resources governed through community-defined rules, have enabled higher reuse rates, more equitable allocation, and greater resilience to changing demand.

Operational experience indicates that commons-oriented governance models are most effective when accompanied by clear rules for use, maintenance, reassignment, and accountability. Such models shift emphasis from ownership to stewardship, enabling devices to circulate over time while remaining embedded in local social and institutional structures.

These governance models directly address power asymmetries between vendors, donors, buyers, refurbishers, and communities by relocating control over devices, maintenance, and lifecycle decisions.

4.4. Transparency, Traceability, and Trust across the Lifecycle

Trust among donors, refurbishers, community organisations, and users has repeatedly emerged as a prerequisite for scalable and sustainable reuse ecosystems. In practice, this trust is strengthened through transparent and traceable device lifecycle management, including documented diagnostics, data sanitisation, refurbishment steps, and transfer histories.

Digital traceability systems, particularly when open and interoperable, support accountability, enable impact assessment, and reduce friction among participating actors. They also allow communities and institutions to demonstrate responsible handling of devices, which in turn facilitates continued donations and institutional support.

4.5. Repairability and Lifecycle Extension as Environmental and Social Strategy

Repair, refurbishment, and refunctionalisation are not merely technical activities, but strategic interventions with both environmental and social implications. Extending device lifecycles reduces e-waste, lowers demand for new hardware production, and mitigates environmental harm associated with extraction and disposal.

At the same time, these activities create opportunities for skill development, employment, and local value creation. Operational experience suggests that prioritizing reuse over premature recycling or destruction yields the greatest combined environmental and social benefits, provided that data protection and safety requirements are adequately addressed.

4.6. Privacy and Security Embedded in Reuse Workflows

Reuse workflows introduce specific privacy and security risks, particularly related to residual data, firmware integrity, and unauthorised access to device inventories. Deployments that treat privacy and security as integral components of refurbishment processes, rather than as afterthoughts, are more successful in maintaining trust and protecting users.

In practice, this includes systematic data sanitisation, clear chain-of-custody procedures, controlled access to lifecycle records, and, where appropriate, mechanisms to detect tampering or misconfiguration. Embedding these considerations early reduces downstream risks and reinforces the legitimacy of reuse initiatives and trust in them.

4.7. Environmental Responsibility across the Full Device Lifecycle

Environmental responsibility in circular device management extends beyond end-of-life recycling. Operational experience highlights the importance of considering environmental impacts across the entire lifecycle, including procurement decisions, refurbishment practices, logistics, and final disposal.

Initiatives that integrate environmental considerations throughout the lifecycle—rather than focusing solely on waste management—are better aligned with broader sustainability goals and regulatory frameworks. This integrated perspective also supports more accurate assessment of environmental benefits, such as avoided emissions and reduced material extraction.

4.8. Community-rooted Governance and Social Relevance

Finally, sustained impact depends on grounding device management and connectivity initiatives in local governance structures and social priorities. Deployments that involve communities in decision-making, regarding allocation, acceptable use, maintenance responsibilities, and future evolution, are more likely to produce socially relevant and durable outcomes.

Operational experience underscores that “meaningful connectivity” is context-dependent: its value emerges from alignment with local practices, cultural norms, and collective aspirations. Community-rooted governance enables initiatives to adapt over time, respond to feedback, and remain relevant beyond initial deployment phases.

5. Operational Practices

5.1. Digitalised Circular Device Management

Observed circular device management systems typically include:

- * Unique device identification (e.g., labels/QR codes) and lifecycle records;
- * Structured triage, diagnostics, and condition grading;
- * Secure data sanitisation steps recorded in device logs;
- * Chain-of-custody tracking across donors, refurbishers, and recipient organisations and end-user persons;
- * Interoperability with other inventory and infrastructure systems (e.g., enterprise resource planning systems, device registries, or network asset registries) where beneficial;
- * Support for processing large-volume device donations or procurement across multiple refurbishers to improve throughput, quality control, and traceability;
- * Optional tamper-evident or cryptographically verifiable logging mechanisms for accountability in multi-stakeholder ecosystems.

Several deployments supporting these practices rely on open-source software tooling for device inventory, diagnostics, and lifecycle tracking. Such tools enable adaptation by different organisations and communities while supporting transparency, quality assurance in refurbishment processes, and the ability to scale device reuse operations across multiple actors.

Together, these lifecycle-management capabilities enable transparency and coordinated reuse circuits where donors, refurbishers, community and formal local organisations, and beneficiary programmes can operate with shared visibility and responsibilities.

5.2. Repair, Training, and Capacity Building

Effective programmes typically:

- * Distinguish between specialised refurbishing tasks (diagnosis, repair, sanitisation, refurbishment) and community-level access/accompaniment functions;
- * Provide training that combines basic hardware diagnostics and repair (electronics), locally sourced spare parts, operating system and application installation and configuration (software), and practical repair and maintenance tasks;
- * Use accessible pedagogies that reduce barriers for youth, women, and marginalised populations;
- * Integrate digital literacy and social inclusion objectives (education, employability, access to services);
- * Provide pathways for income generation or employment (e.g., social enterprises, cooperatives, paid refurbishment);
- * Use digital traceability systems to compute environmental indicators (e.g., avoided e-waste, estimated CO savings) and social indicators (e.g., beneficiary counts, institutions served), reinforcing accountability for donors, policymakers, and communities.

5.3. Alignment with Connectivity Infrastructure

Device reuse is most effective when coordinated with connectivity infrastructure deployments through:

- * Including network equipment (routers, switches, antennas, access points) in lifecycle tracking where relevant;
- * Aligning device availability with connectivity provision (so devices reach users and institutions that can connect);
- * Supporting local repair and reconfiguration of networking equipment where feasible;

- * Tracking performance and replacement cycles to reduce downtime and avoid stranded access infrastructure.

This document does not assume the presence of a specific connectivity infrastructure. The practices described apply to contexts where connectivity is provided through a variety of deployment models, including commercial, community-driven, institutional, or other locally relevant arrangements.

5.4. Community-centred Meaningful Connectivity

Connectivity initiatives may:

- * Engage communities in defining meaningful use for them (education, work, health, services, civic participation, cultural expression, etc.);
- * Combine devices, skills development, and governance to build holistic digital ecosystems;
- * Support shared facilities (community centres, libraries, schools) and collective access models where appropriate, rather than assuming all access is under individual ownership;
- * Design for social inclusion: enable participation of underrepresented groups (women, minorities, youth, adults), account for cultural and linguistic diversity, and empower communities to use connectivity for their own goals (education, civic engagement, small-scale enterprises, local content creation, environmental monitoring, etc.);
- * Respect local agency and context, enabling adaptation of workflows and priorities over time;
- * Include feedback loops and governance mechanisms to evolve deployments according to expressed community needs.

5.5. Collective Access and Commons-based Device Governance

Where appropriate, communities may treat devices as a shared commons. Implementations of collective access typically include:

- * Assigning use-rights instead of permanent ownership to individuals or organisations;
- * Allowing devices to circulate across multiple users and community spaces over time;

- * Establishing clear governance rules for allocation, maintenance responsibilities, reassignment, and end-of-life decisions;
- * Using open-source digital tools to track device history, condition, transfers, and responsible recycling;
- * Embedding accountability mechanisms so actors (donors, refurbishers, community managers) can verify device provenance and lifecycle steps.

This model has been validated operationally in reuse ecosystems and formalised in prior research [Roura2025].

5.6. Federated Registries and Cross-community Coordination

Federated device registries may be used to coordinate reuse across organisations and regions while preserving local governance. Operationally, such federated registries can function similarly to inventory coordination systems used in other circular-economy sectors (e.g., automotive parts reuse), where distributed inventories are searchable across multiple organisations. This allows participating actors to discover available devices, coordinate refurbishment workflows, identify substitute components, and estimate demand for spare parts or devices across regions. Such registries can support:

- * Distributed metadata sharing and device lookup;
- * Cross-organisational coordination for batches and surplus devices;
- * Shared accountability while avoiding centralised control;
- * Federation across communities with different legal, operational, or cultural contexts;
- * Multi-stakeholder governance.

Federation is essential when devices flow across regions, institutions, and countries.

5.7. Secure Data Sanitisation

When devices are refurbished for reuse, data sanitisation should follow recognised good data sanitisation practices such as ITU-T L.1081 [ITU-T-L1081]. Implementers select and apply appropriate methods (e.g., clear, purge, or destruct) depending on media type and sensitivity, before reuse or redistribution.

Implementations should maintain documented chain-of-custody logs and sanitisation records (preferably digitally linked to device lifecycle entries) to provide verifiable proof of data erasure, increase donor trust, and protect privacy.

Where feasible, refunctionalisation (refurbishment and reuse) is preferred over destruction, consistent with circular economy and environmental sustainability goals [ITU-T-L1081].

5.8. Architectural Considerations for Connectivity Infrastructure

The practices described in this document imply architectural considerations relevant to GAIA research, including:

- * Device availability as part of the connectivity architecture, not an external dependency.
- * Device availability, lifecycle management, and governance mechanisms influence the long-term sustainability and autonomy of connectivity infrastructures.
- * Federated registries as a decentralised control-plane component for device lifecycle management and accountability (verifiability).
- * Alignment between network deployment lifecycles and device lifecycles.
- * Reduction of centralised/remote dependencies through local maintenance and governance.

These considerations may inform future research on connectivity architectures, operational sustainability, and resilient deployment models for underserved and community-centred connectivity infrastructures.

6. Human Rights, Security, Privacy, and Sustainability Considerations

Consistent with [RFC8280] and [RFC9620], this section identifies how the operational practices described here can be understood as affecting human rights outcomes through their influence on connectivity, agency, sustainability, and autonomy at the device and infrastructure layer.

6.1. Human Rights

Device availability and governance affect:

- * The ability of individuals and communities to access and benefit from the Internet and from meaningful connectivity;
- * Autonomy and self-determination through repairability, reuse, and local capacity;
- * The right to privacy and data protection in shared or reused devices;
- * Environmental justice in communities impacted by resource extraction and e-waste.

These effects arise through operational risk vectors, including:

- * Limited availability of functional devices leading to constrained access and informational agency;
- * Inadequate data sanitisation creating exposure to unauthorised data disclosure;
- * Non-repairable or vendor-locked devices reducing autonomy and local self-determination;
- * Inequitable disposal practices contributing to environmental harm for vulnerable groups.

Circular device management practices mitigate risks associated with:

- * Data leaks resulting from inadequate data sanitisation;
- * Surveillance risks arising from persistent identifiers, firmware, or misconfigured software;
- * Exclusion caused by vendor lock-in or non-repairable hardware;
- * Unsafe, informal, or inequitable disposal of electronic waste.

By documenting operational practices that address these dimensions, this document contributes deployment-based evidence to ongoing IRTF efforts to integrate human rights considerations into Internet-related research and practice.

6.2. Security

Security risks include:

- * Tampered with or compromised devices;

- * Malicious firmware;
- * Insufficient data erasure;
- * Unauthorised access to device details in inventories and registries;
- * Forged or altered device histories.

These risks can undermine trust in reuse ecosystems and shared devices, and directly reduce access sustainability.

Recommended mitigations include:

- * Verified testing and refurbishment workflows;
- * Secure firmware reinstallation and configuration baselines;
- * Cryptographic or tamper-evident logging where appropriate;
- * Role-based access control for lifecycle systems;
- * Periodic auditing and peer-review among participating organisations.

6.3. Privacy

Reuse systems should apply:

- * Data minimisation and least-privilege access;
- * Local-first and decentralised architectures;
- * Strong sanitisation and verification practices;
- * Transparent documentation of data handling;
- * Encryption for sensitive metadata where stored or transferred.

Device identifiers should be abstracted or scoped appropriately when feasible to reduce long-term cross-context correlation risks. Lifecycle traceability introduces a design tension between transparency and privacy. While device identifiers and lifecycle records support accountability, auditing, and reuse coordination, poorly designed traceability systems may enable unintended tracking or surveillance. Implementations should therefore minimise exposure of persistent identifiers, limit access to lifecycle metadata through appropriate governance and access controls, and use scoped or pseudonymous identifiers where feasible.

6.4. Environmental and Sustainability

Circular device management reduces [Roura2026]:

- * Demand for new hardware;
- * Raw material extraction;
- * CO emissions, land and water pollution from manufacturing;
- * e-waste in vulnerable communities;

while also contributing to economic inclusion by creating financial opportunities, increasing economic independence, and supporting sustainable income sources.

Reuse and refurbishment (after secure sanitisation) should be prioritised over disposal. By enabling safe refunctionalisation of devices that would otherwise be discarded, communities reduce e-waste and environmental harm, consistent with circular economy principles and L.1081 guidance that supports reconditioning over destruction [ITU-T-L1081].

7. Deployment Case Studies (Informative)

This section describes deployments by [EREUSE] in Spain, [EKOA-UNLP] and [TAU-RAEE] in Argentina, and [HAHATAY] in Senegal that illustrate how these practices are applied in diverse contexts.

7.1. Catalonia and Madrid (Spain): eReuse.org ecosystem and social enterprises

The eReuse.org ecosystem coordinates reuse circuits that connect donors (public and private organisations), social refurbishers, recyclers, community organisations, and beneficiaries [EREUSE]. Typical operational characteristics include:

- * Intake of unused devices through institutional volume donation channels;
- * Structured diagnostics, refurbishment, and grading by social enterprises;
- * Digital lifecycle traceability through open-source inventory tooling, supporting transparency and accountability;
- * Allocation of refurbished devices to individuals and organisations through models that may include subsidised pricing, sponsorship, and collective access arrangements;
- * Measurement approaches that support reporting of environmental and social outcomes (e.g., devices reused, avoided e-waste, beneficiary reach).

eReuse deployments also experiment with collective access and ownership: devices may remain part of a shared pool and be redistributed as needs evolve, rather than being permanently assigned to individuals, increasing reuse cycles and long-term availability [Roura2025].

7.2. La Plata (Argentina): EKOA/UNLP programmes integrating refurbishment, training, and outreach

EKOA at the National University of La Plata (UNLP) operates university-linked initiatives that integrate refurbishment, training, and outreach [EKOA-UNLP]. EKOA manages its own production plant for refurbished technological equipment. Observed characteristics include:

- * Involves students, faculty, non-teaching staff, researchers, and extension practitioners linked to university ecosystems, who perform activities within and outside the e-waste management and refurbishment plant, including diagnostics, repair, refunctionalisation, and data sanitisation.
- * Refurbished devices are distributed to schools at all levels, community kitchens and food distribution centres, NGOs, hospitals, health centres, fire brigades, social organisations, university students, Indigenous communities, migrants, older adults, and other vulnerable communities. Devices are typically delivered under loan-for-use (commodatum) or chain-of-custody arrangements.

- * The plant serves as a reception and training site for students from technical secondary schools and universities, who engage in training activities, work-based learning experiences, and student projects.
- * The plant is also a training space for cooperatives of urban recyclers, empowering youth and adults with practical skills across the device and WEEE management chain.
- * Training activities are organised with equitable participation across genders.
- * Environmental responsibility is integrated through secure channels across the WEEE management chain and promoted to donors and beneficiaries of refunctionalised devices.
- * Device reuse is generally linked to digital literacy programmes and territorial initiatives that provide benefits to the wider community (e.g., hospitals, fire brigades, public services).
- * The initiative includes environmental education projects aimed at primary and secondary schools.

7.3. Hahatay (Senegal): Device availability and inclusion in rural and peri-urban contexts

The Hahatay initiative addresses device scarcity in rural and peri-urban contexts where new hardware can be unaffordable or unavailable [HAHATAY]. Observed characteristics include:

- * Sourcing and reusing devices as a practical prerequisite to meaningful connectivity;
- * Integration with community programmes that support digital literacy and community benefit;
- * Emphasis on locally appropriate maintenance and operational continuity.

These contexts highlight the importance of aligning connectivity infrastructure plans with device availability and repair capacity to avoid stranded infrastructure.

7.4. Rosario (Argentina): TAU/RAEE and territorial programmes in villas

TAU/RAEE operates a community-embedded ecosystem in and around Rosario [TAU-RAEE]. A specialised cooperative (TAU) carries out the technical processes of diagnostics, repair, data sanitisation, refurbishment, and e-waste management, while community centres and territorial programmes focus on access, accompaniment, and local participation.

Observed characteristics include:

- * A cooperative of young workers (TAU) manages the e-waste and refurbishment plant where diagnostics, repair, and data sanitisation are carried out.
- * Community centres do not perform the technical refurbishment themselves, but act as coordination and connectivity support points.
- * Training programmes empower youth and adults with practical skills.
- * Refurbished devices are redistributed to schools, families, cooperatives, and social organisations, generally under cession-of-use schemes rather than as permanent donations, including maintenance and replacement, to preserve traceability.
- * Inclusive pedagogical approaches prioritize women and underrepresented groups.
- * Environmental responsibility is integrated through safe recycling channels.
- * Device reuse is connected to digital literacy programmes.

These community-driven refurbishing and connectivity efforts embody community-centred meaningful connectivity: devices and networks are locally governed, refurbishment and reuse are collective, and infrastructure is shaped by community needs and practices, not by vendor-driven or top-down deployment. [GISW2024]

This model demonstrates how circular device management can be sustainably embedded in informal settlements and marginalised communities.

This case illustrates a division of labour model that can be replicated: specialised refurbishers/cooperatives ensure technical integrity and sanitisation, while community organisations ensure access, inclusion, and community-centred governance.

8. Replication Guidelines

Organisations seeking to replicate these practices should consider:

- * Establishing partnerships among donors, specialised refurbishers, community organisations, and (where relevant) connectivity infrastructure operators;
- * Deploying open-source, interoperable inventory tooling to enable traceability and accountability;
- * Developing training pathways (diagnostics, software installation/configuration, repair, sanitisation, responsible e-waste handling);
- * Selecting appropriate governance models, including collective access to devices where it improves equity and sustainability;
- * Aligning device availability with connectivity provision and local access conditions;
- * Defining privacy and security controls, including sanitisation verification and role-based access to inventories;
- * Establishing impact reporting for environmental and social outcomes to maintain trust and continuous improvement;
- * Complying with WEEE management and refunctionalisation regulations.

9. Implications for Research and Deployment

Operational experience also highlights the importance of capacity building alongside architectural design. Training programmes that integrate device repair, refurbishment, software installation, data sanitisation, and governance practices are critical enablers of sustainable connectivity.

Research communities, including the IRTF GAIA Research Group, may contribute to this area by documenting reusable operational patterns, facilitating knowledge exchange across deployments, and developing resources that connect connectivity architectures with sustainability and repairability considerations.

The practices described in this document suggest that device lifecycle management, repairability, ownership, and governance should be considered integral components of connectivity infrastructures. Future research may explore architectural approaches that integrate device registries, lifecycle transparency and accountability, and community governance mechanisms into connectivity deployments.

Understanding how device ecosystems interact with connectivity infrastructure, community participation, and sustainability objectives may contribute to more resilient and inclusive Internet connectivity models.

10. IANA considerations

This document has no IANA actions.

11. Acknowledgements

The authors thank the participating communities and organisations whose operational experience informed this document, including eReuse.org, with Solidana [SOLIDANCA] and ReutilizaK as member social enterprises, EKO/UNLP, TAU/RAEE, Hahatay, and the community organisations and beneficiaries involved in deployment, training, and reuse circuits.

The authors also acknowledge the contributions of Juan Flores (ReutilizaK), Daniel Florin (Solidana), David Franquesa (eReuse.org), Sergio Gimnez (hahatay.org), and Pedro Vilchez (eReuse.org), whose practical experience and insights informed the development of the practices described in this document.

12. References

12.1. Informative References

- [RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <<https://www.rfc-editor.org/rfc/rfc8280>>.
- [RFC9620] Grover, G. and N. ten Oever, "Guidelines for Human Rights Protocol and Architecture Considerations", RFC 9620, DOI 10.17487/RFC9620, September 2024, <<https://www.rfc-editor.org/rfc/rfc9620>>.

12.2. Informative References

[COMMODATE]

Merriam-Webster.com Dictionary, "Commodate",
<<https://www.merriam-webster.com/dictionary/commodate>>.

[EKO-UNLP]

Universidad Nacional de La Plata, "EKO programme website", <<https://ekoa.unlp.edu.ar/>>.

[EREUSE]

eReuse.org, "eReuse.org initiative website",
<<https://ereuse.org/>>.

[GISW2024]

Association for Progressive Communications (APC),
"Meaningful connectivity: What does 'meaningful' mean in
the context of the Internet?", Global Information Society
Watch (GISWatch), 2024, <<https://gisw.org/en/internet-governance-civil-society-participation-internet-rights/what-does-meaningful>>.

[HAHATAY]

Hahatay Network, "Hahatay community initiatives website",
<<https://hahatay.network/>>.

[IGF-PNMA2024]

Internet Governance Forum Policy Network on Meaningful
Access, "How to Conciliate "Access" with "Meaningful":
Practices from the Community", IGF Output Report, 2024,
<https://www.intgovforum.org/en/filedepot_download/314/28585>.

[ISOC-MC2025]

Internet Society, "What is Meaningful Connectivity?",
October 2025,
<<https://www.internetsociety.org/blog/2025/10/what-is-meaningful-connectivity/>>.

[ITU-T-L1081]

International Telecommunication Union, "Recommendation
ITU-T L.1081: Good practices for the sanitization of the
information storage media in end-of-life ICT user
devices", July 2025,
<<https://www.itu.int/rec/T-REC-L.1081>>.

[ITU-UMC]

International Telecommunication Union, "Universal
Meaningful Connectivity Framework", International
Telecommunication Union, 2022, <<https://www.itu.int/itu-d/sites/projectumc/home/aboutumc/>>.

[Ostrom1990]

Ostrom, E., "Governing the Commons: The Evolution of Institutions for Collective Action", Cambridge University Press, 1990.

[Roura2025]

Roura, M., Navarro, L., and R. Meseguer, "Reuse of ICT devices as commons: a property rights and governance model for collective access", ACM Journal on Computing and Sustainable Societies, 2025, <<https://doi.org/10.1145/3770067>>.

[Roura2026]

Roura, M., Navarro, L., and R. Meseguer, "Assessing the impacts of computer reuse for digital inclusion from product information", Cleaner Production Letters, Volume 10, Article 100123, 2026, <<https://doi.org/10.1016/j.clpl.2025.100123>>.

[SOLIDANCA]

Solidana, "Solidana social enterprise website", <<https://solidanca.cat/>>.

[TAU-RAEE] TAU/RAEE, "TAU Gestin de Residuos de Aparatos

Elctricos y Electrnicos", <<https://tau.org.ar/raee/>>.

Authors' Addresses

Leandro Navarro
ISOC.CAT
Barcelona
Spain
Email: leandro@ereuse.org

Mireia Roura
eReuse.org
Barcelona
Spain
Email: m.roura@ereuse.org

Eduardo Rodriguez
TAU/RAEE
Rosario
Argentina
Email: eduardorodriguez@tau.org.ar

Viviana Ambrosi
EKOA, Facultad de Informtica - UNLP
La Plata
Argentina
Email: viviana.ambrosi@ekoa.unlp.edu.ar