

RÉSEAU DES FEMMES LEADERS POUR LE DÉVELOPPEMENT
RFLD · rflgd.org

Digital Security & Information Management Policy

Device security, secure communications, password management, data classification, and incident response — protecting RFLD's people, data, and mission

Version: 1.0	Effective Date: May 2026
Policy Owner: Data Protection Officer / Executive Director	Document Reference: RFLD-POL-DSIM-v1.0
Approved By: Board of Directors, RFLD	Next Review: May 2027

Cotonou (HQ) · Accra · Dakar · Banjul
admin@rflgd.org · integrity@rflgd.org · finance@rflgd.org

Table of Contents

1. Purpose, Threat Landscape, and RFLD's Digital Security Context
2. Scope, Definitions, and Governing Principles
3. Information Classification Framework
4. Device Security
5. Password and Authentication Management
6. Secure Communications
7. Network and Remote Access Security
8. Data Storage, Handling, and Sovereign Infrastructure
9. Email and Collaboration Tools
10. Cloud Services and Third-Party Platforms
11. Digital Security for Travel
12. Spyware and Advanced Persistent Threats
13. Acceptable Use of RFLD Digital Systems
14. Website, Social Media, and External Digital Presence
15. Incident Response Framework
16. Security Awareness Training
17. Roles and Responsibilities
18. Partner and Third-Party Digital Security
19. Compliance, Audit, and Enforcement
20. Governance and Policy Review
- Annex A — Device Security Checklist
- Annex B — Approved Tools Reference List
- Annex C — Digital Security Incident Report Form
- Annex D — Digital Security Quick Reference Card

1. Purpose, Threat Landscape, and RFLD's Digital Security Context

1.1 Purpose

This Digital Security and Information Management Policy ('the Policy') establishes RFLD's comprehensive framework for protecting its digital systems, data, communications, and — critically — the people whose safety depends on RFLD's digital security practices. It defines mandatory standards for device security, secure communications, password management, information classification, data storage, and digital incident response, applicable to all staff, consultants, Board members, and implementing partners who use RFLD's systems or handle RFLD's data.

Digital security at RFLD is not an IT administration matter — it is a human rights and programme integrity issue. The data RFLD holds includes the identities, locations, affiliations, and communications of women human rights defenders and activists operating in environments where that information, if exposed, could lead to arrest, violence, targeted surveillance, or death. The systems through which RFLD's programme operates are of direct interest to state actors who deploy commercial spyware against civil society. Every RFLD staff member's digital behaviour is therefore a programme security decision, not a personal preference.

1.2 RFLD's Threat Landscape

RFLD operates at a unique intersection of risk: it is both a direct target of potential state surveillance and a custodian of data belonging to activists who are themselves targets. The specific threat vectors RFLD must manage include:

Threat Category	RFLD-Specific Exposure	Risk Level
Commercial spyware (Pegasus, Predator, FinSpy)	State actors in RFLD's programme countries have deployed commercial spyware against civil society. RFLD's programme and staff in direct contact with WHRDs are plausible targets. A single compromised device can expose the entire contact list, communications history, and location data of every person in the RFLD network.	CRITICAL
Targeted phishing and social engineering	Sophisticated phishing campaigns targeting civil society organisations — crafted to appear as donor communications, NGO sector messages, or internal RFLD emails. RFLD staff may be specifically targeted based on public information about their roles.	HIGH
Data breach through misconfigured storage	Unintentional exposure of sensitive programme data through misconfigured cloud storage, improperly shared documents, or inadequate access controls — without any malicious actor involved.	HIGH
Ransomware and destructive malware	RFLD's financial systems, programme data, and helpline records could be targets for ransomware attacks designed either for financial gain or to disrupt civil society operations.	MEDIUM-HIGH
Insider risk	Unintentional data exposure by staff through poor security hygiene; and — rarely — deliberate data leakage. Neither is a reflection on staff character; both require structural controls.	MEDIUM
Interception at border crossings	Forced or coerced access to staff devices during border crossings in programme countries. Particularly relevant for Tier 2, 3, and 4 country travel.	MEDIUM-HIGH
Supply chain compromise	Malicious code embedded in software or tools used by RFLD or its partners — exploiting the trust in established tools to gain access to systems.	MEDIUM

1.3 Integration with RFLD's Policy Framework

This Policy operates alongside RFLD's Data Protection Policy (RFLD-POL-DPP-v1.0), which governs the legal basis, purpose, and individual rights framework for personal data processing. Where both policies apply — as they do for all personal data — the more protective provision governs. This Policy focuses on the technical and operational security controls that protect data regardless of classification; RFLD-POL-DPP-v1.0 governs the legal and rights dimensions. The Risk Management Policy (RFLD-POL-RISK-v1.0 Section 11) governs the risk register treatment of digital security risks.

2. Scope, Definitions, and Governing Principles

2.1 Scope

This Policy applies to all persons who access, process, store, or transmit RFLD data or who use RFLD digital systems — including all permanent, fixed-term, part-time, and probationary staff; Board members; consultants and contractors; volunteers and interns; and implementing partners and sub-grantees to the extent specified in their agreements. It covers all RFLD-owned or RFLD-managed devices, networks, systems, and accounts; all personal devices used to access RFLD data or systems; and all data in RFLD's custody regardless of classification level.

2.2 Key Definitions

Term	Definition
RFLD Digital System	Any device, platform, application, network, or service operated by RFLD or on RFLD's behalf — including email, cloud storage, financial systems, programme management databases, the helpline platform, and the DONÜESË Data Center.
Endpoint	Any device that connects to RFLD's network or accesses RFLD data — including laptops, desktop computers, smartphones, tablets, and USB storage devices.
Multi-Factor Authentication (MFA)	An authentication method that requires two or more independent verification factors — typically a password plus a one-time code sent to a trusted device or generated by an authenticator application.
End-to-End Encryption (E2EE)	Encryption that ensures data is encrypted at the sender's device and can only be decrypted by the intended recipient — the service provider and any intermediary cannot read the content.
VPN (Virtual Private Network)	A service that creates an encrypted tunnel for internet traffic, protecting it from interception on untrusted networks and masking the user's IP address from destination servers.
Phishing	A social engineering attack in which a malicious actor impersonates a trusted entity to deceive the target into revealing credentials, installing malware, or disclosing sensitive information.
Spyware	Commercial or state-developed software covertly installed on a device to surveil the user's communications, locations, and activities without their knowledge. Examples include Pegasus (NSO Group) and Predator (Intellexa).
Zero-Click Exploit	A method of device compromise that requires no action by the target — the malware installs itself through a vulnerability in the device's software without the user clicking a link or opening a file.
Data Sovereignty	RFLD's principle that sensitive programme data — particularly Class 4 data relating to WHRDs and activists — must reside on infrastructure controlled by RFLD or a trusted African civil society entity, not on commercial cloud platforms subject to foreign jurisdiction.
DPO	RFLD's Data Protection Officer — the person responsible for overseeing data protection compliance and digital security governance. Primary contact for all incidents involving personal data.
IT Lead	The person responsible for RFLD's technical infrastructure, device management, and operational digital security controls. Reports to the Executive Director.
Incident	Any event that has compromised or could compromise the confidentiality, integrity, or availability of RFLD's data or systems — whether caused by a malicious actor, human error, or technical failure.

2.3 Governing Principles

Principle	Application at RFLD
People First	The primary objective of RFLD's digital security is the safety of the people — WHRDs, activists, programme participants, and staff — whose data RFLD holds. Technical

Principle	Application at RFLD
	controls exist to serve this objective, not to create compliance burdens.
Security by Design	Digital security is built into systems and processes from the start, not added after the fact. New tools, platforms, and data collection activities are assessed for security implications before adoption.
Least Privilege	Every user, system, and application has access only to the data and functions it genuinely needs — no more. Access is granted explicitly and reviewed regularly.
Defence in Depth	RFLD does not rely on any single security control. Multiple overlapping layers of protection ensure that a failure in one control does not expose data. This is especially critical given the sophistication of spyware threats RFLD faces.
Transparency and No-Blame Reporting	Security incidents are reported promptly and honestly — the culture is one of 'raise it early and fix it together', not 'hide it to avoid blame'. Staff who report incidents promptly are recognised; those who conceal them face consequences.
Proportionality	Security controls are proportionate to the sensitivity of the data and the severity of the threat. The most stringent controls apply to Class 4 (HIGH RISK) data involving WHRD and activist identities. Less sensitive operational data carries lighter controls.

3. Information Classification Framework

3.1 Why Information Classification Matters

Not all RFLD information carries the same risk profile. A published programme report and a database of WHRD identities require completely different handling. Information classification provides a consistent, organisation-wide framework for determining what level of protection any given piece of information requires — based on what harm would result from its unauthorised disclosure, modification, or loss. Every RFLD staff member must be able to identify the classification of the information they handle and apply the correct handling rules.

3.2 RFLD's Four-Level Classification System

Class	Label	Definition	Examples	Harm If Disclosed
1	PUBLIC	Information intended for public access or that poses no harm if disclosed. Approved for external sharing.	Published reports; website content; public advocacy statements; published research.	None — public by design.
2	INTERNAL	Information for RFLD operational use. Not harmful if disclosed but not intended for public sharing. Default classification for general operational information.	Meeting agendas; internal reports; staff contact lists; operational budgets; general programme plans.	Minor reputational or operational inconvenience. No individual harm.
3	CONFIDENTIAL	Information that, if disclosed without authorisation, could harm RFLD's institutional interests, donor relationships, or the interests of individual staff or partners. Restricted to those with a genuine need to know.	Unpublished financial data; personnel records; donor proposals and grant agreements; partner performance assessments; internal investigations; legal correspondence.	Significant institutional harm; reputational damage; potential harm to individuals named.
4	HIGH RISK	Information whose unauthorised disclosure could directly cause serious harm to identifiable individuals — physical danger, arrest, harassment, or persecution.	WHRD and activist identities, locations, and affiliations; helpline case records; safeguarding incident reports; individual political affiliation data in repressive contexts; real-time location data of staff in Tier 3–4 countries.	Life-threatening or freedom-threatening harm to real people.

3.3 Classification Responsibilities

The person who creates or receives information is responsible for assigning the correct classification at the point of creation or receipt. Where classification is unclear, the DPO is consulted. The default classification — when in doubt — is Class 3 (Confidential). A staff member who cannot determine whether information is Class 3 or Class 4 should assume Class 4 and treat it accordingly, then seek clarification from the DPO.

3.4 Handling Rules by Classification Level

Class	Storage	Transmission	Access	Disposal
1 — Public	Any approved system	Any channel	No restrictions	Standard deletion

Class	Storage	Transmission	Access	Disposal
2 — Internal	RFLD-approved systems; no personal accounts	RFLD email or approved platforms	All staff with relevant role	Secure deletion; shredding for physical
3 — Confidential	RFLD-approved systems; access-controlled; encrypted at rest	Encrypted channels only; RFLD VPN for remote access	Named authorised individuals only; access reviewed quarterly	Secure deletion (NIST-compliant); shredding for physical; DPO sign-off
4 — HIGH RISK	ONLY Data Center or equivalent RFLD-approved sovereign infrastructure only; full encryption; air-gapped backup	End-to-end encrypted channels only; never via standard email; never via commercial cloud	Strictly limited to persons with documented operational need; DPO and IT Lead authorise each access grant	Cryptographic erasure; DPO sign-off; destruction record retained

3.5 Labelling Requirements

Class 3 and Class 4 documents must be labelled clearly at the top and bottom of every page. Digital files must include the classification label in the filename or document header. Class 4 files must additionally include a handling warning: 'CLASS 4 — HIGH RISK — Do not copy, forward, or share without DPO authorisation.'

4. Device Security

4.1 Endpoint Security Standards — Mandatory for All RFLD Devices

The following standards apply to every device owned or managed by RFLD — laptops, desktop computers, smartphones, and tablets — as well as to any personal device used to access RFLD Class 2, 3, or 4 data or systems. The IT Lead audits device compliance quarterly using the Device Security Checklist (Annex A).

Security Control	Standard	Rationale
Operating System Updates	Critical and high-severity security patches must be applied within 14 days of release. OS auto-update must be enabled where available. EOL (end-of-life) operating systems are not permitted on RFLD systems.	Unpatched vulnerabilities are the most common entry point for malware, including commercial spyware.
Full-Disk Encryption	All RFLD device storage must be encrypted using the device's native full-disk encryption (BitLocker for Windows; FileVault for macOS; device encryption on Android and iOS). Encryption keys are managed by the IT Lead.	Protects data if a device is lost, stolen, or seized. A stolen encrypted laptop reveals nothing without the decryption key.
Screen Lock	All devices must lock automatically after a maximum of 5 minutes of inactivity. PIN, passphrase, or biometric authentication required to unlock. Must be activated before any RFLD account or data is accessed.	Prevents opportunistic access when a device is left unattended.
Approved Anti-Malware	RFLD's approved anti-malware solution (specified in Annex B) must be installed and active on all laptops and desktops. Real-time protection enabled. Definitions updated automatically within 24 hours of release.	Detects known malware — including some spyware variants — before it executes.
Mobile Device Management (MDM)	All RFLD-issued smartphones and tablets must be enrolled in RFLD's MDM system. MDM enables remote wipe in case of loss, theft, or confirmed compromise.	Remote wipe is the fastest way to protect Class 4 data when a device is lost or compromised.
Application Installation	On RFLD-issued devices, only applications approved by the IT Lead may be installed. Staff may not install software from unofficial sources (outside official app stores) on any RFLD device.	Unofficial applications are a primary delivery mechanism for malware and spyware.
Jailbreaking / Rooting Prohibition	RFLD devices must not be jailbroken or rooted. Any RFLD-issued device found to be jailbroken is immediately withdrawn from service and the incident investigated.	Jailbreaking/rooting removes the operating system's security controls, making the device trivially vulnerable.
USB and External Storage	USB storage devices (flash drives) may only be connected to RFLD laptops or desktops if they are RFLD-issued and scanned by the IT Lead before first use. Personal USB drives are not permitted on RFLD devices.	USB devices are a classic malware delivery vector — including in targeted attacks against civil society.

4.2 Personal Device Policy (BYOD)

RFLD's preference is that staff use RFLD-issued devices for all work activities. Where a staff member uses a personal device to access RFLD Class 2 systems (standard email, scheduling, public documents), the following minimum requirements apply:

- The device must meet the full-disk encryption, screen lock, auto-update, and anti-malware standards above.
- RFLD email must be accessed through a dedicated app (not via an unmanaged browser) that can be remotely de-provisioned.
- Class 3 and Class 4 data may not be stored locally on personal devices under any circumstances.
- Personal devices used for RFLD access must not have jailbreak/root enabled.

Use of personal devices to access Class 3 or Class 4 data requires IT Lead and DPO authorisation in writing, is granted only in exceptional operational circumstances, and is time-limited.

4.3 Lost or Stolen Devices

Any RFLD device that is lost or stolen must be reported to the IT Lead and DPO within 2 hours of discovery. The IT Lead will immediately activate the remote wipe protocol for MDM-enrolled devices. The DPO assesses whether the loss constitutes a data breach requiring notification under RFLD-POL-DPP-v1.0. The staff member completes the Digital Security Incident Report Form (Annex C) within 24 hours.

4.4 Device Lifecycle — Provisioning and Decommissioning

New devices are provisioned by the IT Lead before being issued to staff — with all required security controls installed, configured, and verified. When a device is decommissioned — for any reason including replacement, repair, staff departure, or confirmed compromise — it undergoes a cryptographic erasure process verified by the IT Lead before disposal. Devices containing Class 4 data are physically destroyed after cryptographic erasure. The IT Lead maintains a Device Register — a log of all RFLD-issued devices with: device type; serial number; assigned user; issue date; and decommissioning date and method.

5. Password and Authentication Management

5.1 The Password Problem — And RFLD's Solution

Weak, reused, or stolen passwords are the single most common cause of account compromise. The traditional advice to 'remember complex passwords' has been largely discredited — it produces either weak passwords that are memorised or strong passwords written on sticky notes. RFLD's approach is different: use a password manager to generate and store strong, unique passwords for every account, and use Multi-Factor Authentication (MFA) to make stolen passwords useless on their own.

5.2 Password Standards

Standard	Requirement
Minimum Length	Minimum 16 characters for all RFLD system passwords. A passphrase of four or more random words (e.g., 'purple-forest-tide-eleven') is equally acceptable and often more memorable than a character-substitution password.
Uniqueness	Every RFLD account must have a different password. Reusing a password across accounts means a single breach compromises multiple systems. No exceptions.
Password Manager	All RFLD staff are required to use RFLD's approved password manager (specified in Annex B) to store and generate passwords for all work accounts. Master password for the password manager must be a strong passphrase known only to the staff member.
Password Sharing	Passwords must not be shared between individuals. Where a shared account is operationally necessary (e.g., a social media account), the IT Lead creates a shared vault entry accessible to authorised users — the actual password is generated and managed in the password manager, not known to individuals.
Password Rotation	Passwords are changed: immediately on suspicion of compromise; immediately on staff departure from any role; for shared accounts — quarterly. Regular forced rotation without a security trigger has been removed from RFLD's standard (research shows it reduces security by encouraging weaker passwords).
No Password Storage in Browser	Passwords must not be saved in web browsers — browsers are not secure password managers and are frequently targeted. Use the approved password manager only.
No Password Transmission	Passwords must never be transmitted in plaintext — not by email, not by standard SMS, not by unencrypted messaging. Where a new password must be communicated, use an approved encrypted channel.

5.3 Multi-Factor Authentication (MFA) — Mandatory

MFA is mandatory for all RFLD system accounts without exception. MFA means that even if an attacker obtains a staff member's password, they cannot access the account without also possessing the second factor (typically a time-based one-time code from an authenticator app).

System / Account Type	MFA Requirement	Approved MFA Method
RFLD email (all accounts)	Mandatory	TOTP authenticator app (Aegis, Authy, or Microsoft Authenticator). SMS-based MFA accepted where authenticator app is not technically possible — but is less secure.
RFLD financial systems	Mandatory — hardware token preferred	TOTP authenticator app or hardware security key (FIDO2/WebAuthn). SMS not accepted for financial system MFA.
Helpline platform and case management	Mandatory — highest priority	Hardware security key required for all accounts with access to Case 4 helpline data. Authenticator app as fallback only with DPO approval.
DCNÜESÈ Data Center access	Mandatory	Hardware security key (FIDO2/WebAuthn). No exceptions.

System / Account Type	MFA Requirement	Approved MFA Method
RFLD programme management systems	Mandatory	TOTP authenticator app minimum.
Social media and external platforms	Mandatory where the platform supports it	TOTP authenticator app. SMS accepted where authenticator is not supported.
Personal accounts used for RFLD work	Strongly recommended	TOTP authenticator app.

5.4 MFA Recovery Codes

When MFA is enabled on any RFLD system account, the recovery codes generated by the platform must be: stored in the RFLD approved password manager in the relevant account entry; not stored on the device used to access the account; and never printed and left in the office without a locked storage location. Recovery codes provide full account access without MFA — they are equivalent in sensitivity to the account password.

6. Secure Communications

6.1 Communication Security Tiers

Not all RFLD communications require the same level of security. The level of protection applied to a communication should match the classification of the information it contains. RFLD operates three communication security tiers:

Tier	For Information Class	Required Protection	Approved Tools
Tier A — Standard	Class 1 and 2	Standard RFLD email (TLS-encrypted in transit); approved collaboration platforms with TLS.	RFLD email; approved team collaboration tools (Annex B)
Tier B — Secure	Class 3	End-to-end encrypted messaging; encrypted email where available; RFLD VPN for all remote access.	Signal (approved); encrypted RFLD email with S/MIME; approved secure collaboration workspace.
Tier C — Maximum	Class 4	End-to-end encrypted messaging only; no standard email; no commercial platforms; sovereign infrastructure only; hardware security key authentication.	Signal (approved); RFLD sovereign infrastructure direct access; hardware key authenticated systems only.

6.2 Approved and Prohibited Communication Tools

Tool / Platform	Status	Conditions and Scope of Approved Use
Signal	APPROVED — Tier B/C	Required for all Class 3 and Class 4 communications. Disappearing messages must be enabled for Class 4 conversations — maximum 1 week message retention. 'Note to self' may not be used to store Class 4 data.
RFLD institutional email	APPROVED — Tier A/B	Standard for Class 1 and Class 2 communications. May be used for Class 3 where S/MIME encryption is applied. Never for Class 4 data — not even in encrypted form.
WhatsApp	APPROVED with restrictions — Tier A only	Standard operational communications (scheduling, logistics) and Class 1/2 content only. Not approved for Class 3 or Class 4 data. WhatsApp metadata (who contacts whom, when, from where) is retained by Meta and is a surveillance risk in some programme contexts.
Wire / Element (Matrix)	APPROVED — Tier B/C	Approved for use with WHRDs and programme partners who cannot use Signal. End-to-end encrypted. DPO approval required for Class 4 use.
Gmail / Google Workspace personal	PROHIBITED for Class 2+	Not an approved RFLD tool. Personal Gmail accounts must not be used for any RFLD work communications. RFLD data in personal Gmail is outside RFLD's data governance and is subject to Google's terms and surveillance risk.
Facebook Messenger / Instagram DM	PROHIBITED for any RFLD data	Not end-to-end encrypted by default. Owned by Meta. Significant metadata retention. Not approved for any RFLD programme communication.
Telegram	PROHIBITED for Class 3+	Not end-to-end encrypted by default (only in 'secret chats'). Group chats are not E2EE. Not approved for Class 3 or Class 4. May be used for Class 1 public channel content only.
SMS / standard voice call	RESTRICTED — Class 1 emergency only	Plaintext SMS and unencrypted calls are not secure. Approved only for basic logistics and emergency check-ins where no secure alternative is available. Never used for programme content.

6.3 Email Security Standards

- All RFLD email is sent from @rflgd.org accounts. Staff must not use personal email accounts for RFLD communications involving Class 2 or higher information.
- Email attachments containing Class 3 data must be password-protected before attachment, with the password communicated via a separate secure channel.
- Class 4 data must never be sent by email — not even in encrypted or password-protected form. The attack surface for email (phishing, forwarding, archiving) is too broad for Class 4 material.
- Suspicious emails — particularly those requesting credential input, containing unexpected attachments, or appearing to be from known contacts but with unusual content — must be reported to the IT Lead without clicking any links or opening attachments.

7. Network and Remote Access Security

7.1 Office Network Security

RFLD's office networks in all four offices are maintained by the IT Lead with the following minimum standards:

- Wi-Fi networks use WPA3 encryption (or WPA2-AES as minimum where WPA3 is not supported).
- Staff and guest networks are segregated — visitors and untrusted devices use a separate guest network that cannot access RFLD internal systems.
- Network routers and switches have default passwords changed and are updated to current firmware quarterly.
- Office network access logs are retained for 90 days and reviewed by the IT Lead monthly.

7.2 VPN — Mandatory for Remote Access

RFLD's approved VPN (see Annex B) must be active before accessing any RFLD system from outside an RFLD office network. This is non-negotiable. There are no exceptions for home networks, trusted personal networks, or hotel networks. 'It's probably fine' is not an acceptable security assessment — sophisticated surveillance can operate on any network. VPN activation is the first action before any RFLD work begins outside the office.

Specific VPN requirements:

- Kill switch: RFLD's VPN must have a kill switch enabled — automatically disconnecting internet access if the VPN connection drops, rather than continuing over an unprotected connection.
- No split tunnelling: All traffic must be routed through the VPN while it is active — not just RFLD system traffic.
- VPN credential security: VPN credentials are distinct from other RFLD system passwords, stored in the password manager, and protected by MFA.

7.3 Public and Untrusted Networks

Public Wi-Fi — in cafés, hotels, airports, conference venues, and public spaces — must be treated as hostile. The following rules apply when using public networks:

- VPN must be activated before any RFLD system access.
- No RFLD login screens should be visible to anyone who could see the screen — use a privacy screen filter or reposition.
- In Tier 3 and Tier 4 countries: public Wi-Fi networks must not be used for any RFLD work communications — mobile data with VPN is preferred.
- Hotspots created from personal mobile phones are treated as public networks — VPN applies.

8. Data Storage, Handling, and Sovereign Infrastructure

8.1 Data Residency Principles

Where RFLD data resides determines who can be compelled to disclose it, who has administrative access to it, and whether RFLD can maintain control over it in a crisis. RFLD applies the following data residency rules:

Class	Permitted Storage Infrastructure	Prohibited Storage	Rationale
1	Any approved platform including public cloud	No specific prohibition	Public information — no restriction
2	RFLD-approved systems; RFLD-managed servers; approved cloud platforms listed in Annex B	Personal accounts; unapproved cloud services	Internal operational data should be controlled but is not life-safety sensitive
3	RFLD-managed encrypted storage; approved Class 3-certified cloud services; local encrypted storage on RFLD devices	Personal cloud accounts (iCloud, Google Drive, Dropbox); unencrypted local storage on unmanaged devices	Confidential data requires access control and audit trail that personal accounts cannot provide
4 — HIGH RISK	RFLD DŌNŪESĚ Data Center exclusively; or approved sovereign civil society infrastructure with equivalent security posture. Full encryption at rest. Air-gapped backup	Any commercial cloud platform; any non-RFLD server; personal accounts; unencrypted storage on any device	Life-safety data cannot be subject to commercial platform jurisdiction, law enforcement requests through commercial providers, or commercial data breaches. Sovereign control is non-negotiable.

8.2 The DŌNŪESĚ Data Center

RFLD's DŌNŪESĚ Data Center is its primary sovereign data infrastructure — hosted in West Africa, under RFLD's control, not subject to foreign legal jurisdiction or commercial cloud platform terms of service. All Class 4 data is stored on the DŌNŪESĚ Data Center exclusively. Access to the Data Center requires hardware security key authentication. The IT Lead maintains the Data Center's technical security; the DPO maintains its data governance. The Data Center architecture is reviewed annually by the IT Lead and DPO. Any proposed migration, replication, or connection of DŌNŪESĚ data to external systems requires DPO and Executive Director approval.

8.3 Data Backup and Recovery

RFLD's critical data systems are backed up according to the following schedule and tested quarterly:

- Class 3 systems: Daily automated backup; weekly full backup; monthly restoration test; 30-day backup retention.
- Class 4 systems (DŌNŪESĚ): Daily automated encrypted backup to a physically separate air-gapped location; weekly restoration test; 90-day backup retention; backup access requires DPO and IT Lead dual authorisation.
- The backup system is physically separate from the primary system — a ransomware attack on the primary system cannot propagate to the backup.

9. Email and Collaboration Tools

9.1 RFLD Email System

RFLD's institutional email operates under the @rflgd.org domain. All staff are issued RFLD email accounts for work use. The email system is configured with:

- TLS encryption for email in transit between mail servers.
- SPF, DKIM, and DMARC authentication records to reduce the risk of RFLD email being spoofed in phishing attacks.
- Email archiving for compliance with donor audit and national law retention requirements.
- Anti-spam and anti-malware scanning of all incoming attachments and links.

9.2 Email Handling Rules

- Suspicious emails: Report immediately to the IT Lead — do not click links, open attachments, or reply. Use the 'Report Phishing' function if available, or forward as an attachment to the IT Lead.
- External link safety: Hover over links before clicking to verify the destination URL. Use a link-checking tool (specified in Annex B) for suspicious links. When in doubt, do not click.
- Bulk or broadcast email: Mass emails to external lists must be sent through RFLD's approved email marketing tool — not from individual RFLD accounts — to maintain list quality and RFLD's sender reputation.
- Email account security: The RFLD email account is protected by a unique strong password and MFA. Email must be accessed through the approved RFLD email app or RFLD web client — not through personal email clients without IT Lead approval.

9.3 Collaboration and Document Sharing

RFLD's approved document collaboration and sharing platforms are specified in Annex B. The following principles apply regardless of platform:

- Shared links to Class 3 or Class 4 documents must require authentication — no open public links.
- Access to shared documents is reviewed quarterly by the IT Lead — removing access for staff who have changed roles or left RFLD.
- Class 4 documents are not shared via any collaboration platform. They are accessed directly on the DONUESE Data Center.
- Version control: For critical operational documents, version history must be enabled so that modifications can be traced and reverted if necessary.

10. Cloud Services and Third-Party Platforms

10.1 Cloud Adoption Review

Before adopting any new cloud service or third-party platform for RFLD work, the IT Lead and DPO must conduct a Cloud Security Assessment. The assessment evaluates:

- The jurisdiction of the platform's data centres and the applicable law for data requests.
- The platform's encryption standards — at rest and in transit.
- The platform's track record on data breach transparency and security incident response.
- Whether the platform's terms of service are compatible with RFLD's obligations to its programme participants.
- The maximum classification of RFLD data that the platform is approved to store.

New tools are not adopted for work use until the assessment is complete. The approved tool list (Annex B) is updated when new tools are approved or existing approvals are withdrawn.

10.2 Shadow IT Prohibition

Shadow IT — using unapproved tools for work purposes because they are convenient, familiar, or free — is a significant security risk. Examples include: using personal Google Drive to share a programme document; using a personal Dropbox account to store a field report; using a free online translation tool that stores input data. All RFLD work data must reside in and be processed by RFLD-approved tools only. Staff who identify a tool that is not on the approved list but would serve a genuine operational need should request IT Lead assessment — not simply start using it.

11. Digital Security for Travel

11.1 Pre-Travel Digital Security Assessment

Before any international travel, the traveller completes a digital security review as part of the Pre-Travel Security Briefing (Travel Policy Annex D / RFLD-POL-TEX-v1.0 Section 12.2). The digital security review specifically confirms:

- Device data minimisation: Class 4 data removed from travel devices. Class 3 data limited to what is operationally necessary.
- VPN is installed, configured, and tested — including kill switch verification.
- Signal is installed and up to date.
- MFA authenticator apps are backed up (recovery codes stored in password manager).
- Device encryption is verified as active.
- Auto-lock is set to 2 minutes maximum for travel devices (tighter than standard).
- Emergency data deletion capability: The traveller knows how to trigger remote wipe via MDM if required.

11.2 Clean Travel Devices

For Tier 2, 3, and 4 country travel, the IT Lead provisions a clean travel device — a device containing only the minimum apps and data needed for the specific mission, with no historical data, no contacts beyond those operationally required, and no connection to RFLD's broader systems. Clean travel devices are:

- Wiped and rebuilt after every high-risk mission before reissue.
- Assessed by the IT Lead for signs of compromise on return from any Tier 3 or Tier 4 mission — before reconnecting to RFLD networks.
- Never connected to RFLD networks on return from a Tier 4 mission without explicit IT Lead sign-off.

11.3 Border Crossing Protocol

Staff crossing international borders — particularly in Tier 2, 3, and 4 countries — should be aware of the following:

- Border authorities in some programme countries may require device inspection or demand access to devices. Staff are not required to resist or refuse such demands — personal safety takes absolute priority.
- If a device is seized or inspected at a border: Do not resist. Remain calm. Note the location, time, and identities of officials involved if safe to do so. Report to the DPO and IT Lead as soon as safely possible.
- The DPO and IT Lead advise on whether Class 4 data should be removed before specific border crossings — this is assessed on a per-mission basis as part of the security briefing.
- Biometric device unlocking (fingerprint, face ID) may be compelled by some legal systems with less legal protection than passcode access. Staff travelling to Tier 3 or 4 countries should consider disabling biometric unlock before border crossings.

12. Spyware and Advanced Persistent Threats

12.1 The Spyware Threat to RFLD

Commercial spyware — tools like Pegasus (NSO Group), Predator (Intellexa/Cytrox), and FinSpy (FinFisher) — have been documented attacking civil society organisations and human rights defenders in West and Central Africa and across RFLD's programme region. These tools are sold to governments, exploit zero-day vulnerabilities that cannot be prevented by standard anti-malware, and can silently access everything on a compromised device: messages, calls, emails, contacts, location, camera, and microphone.

12.2 Why Standard Anti-Malware Is Insufficient

Standard anti-malware tools detect known malware signatures — they are largely ineffective against novel commercial spyware that exploits zero-click vulnerabilities unknown to security software vendors. RFLD does not rely on anti-malware as its primary defence against spyware. The primary defences are:

- Lockdown Mode (Apple devices): For staff with elevated spyware risk — including helpline staff, the DPO, and the Executive Director — Apple Lockdown Mode must be enabled on iPhone and Mac devices. Lockdown Mode significantly restricts the attack surface available to spyware at the cost of some functionality.
- OS patch urgency: Zero-click exploits typically abuse recently disclosed vulnerabilities. Applying security patches within 14 days (or within 48 hours for patches addressing actively exploited vulnerabilities) is critical.
- Regular device audits: The IT Lead, in coordination with RFLD's digital security advisory network, audits high-risk staff devices for indicators of compromise using Mobile Verification Toolkit (MVT) or equivalent tooling — at minimum annually and after any suspected compromise.
- Network traffic monitoring: Unusual outbound data transfers from RFLD devices can indicate active compromise. The IT Lead monitors RFLD office network traffic for anomalies.
- Separation of high-risk functions: The helpline, WHRD case management, and programme participant data handling are conducted on dedicated systems physically and logically separated from RFLD's general administrative systems.

12.3 Signs of Potential Device Compromise

Staff should report any of the following to the IT Lead and DPO immediately — these may be indicators of spyware infection:

- Device battery draining significantly faster than usual without explanation.
- Device running unusually hot without intensive use.
- Increased mobile data usage without a corresponding change in usage patterns.
- Unusual device behaviour — apps opening without input; screen illuminating spontaneously; microphone or camera indicator activating unexpectedly.
- Unexpected device reboots.
- Messages, emails, or calls not sent by the staff member appearing to have been sent from their device.
- Receiving an unusual notification about a failed login to an account from an unfamiliar location.

Staff must not attempt to investigate a suspected compromise themselves — they risk destroying forensic evidence. The correct action is to stop using the device, keep it powered on (not to destroy evidence), contact the IT Lead immediately, and follow the Incident Response Protocol (Section 15).

12.4 Response to Confirmed Spyware Compromise

Where a device is confirmed or strongly suspected to have been compromised by commercial spyware:

1. The device is immediately isolated from all RFLD networks — physically disconnected and not reconnected until cleared by the IT Lead.
2. The DPO and Executive Director are notified within 1 hour.

3. The Board Chair is notified within 24 hours — a confirmed spyware compromise of an RFLD device is a Critical risk under RFLD-POL-RISK-v1.0.
4. A forensic copy of the device is taken (by the IT Lead or an engaged specialist) before any remediation action, to preserve evidence.
5. Relevant passwords are changed immediately from a clean uncompromised device.
6. The affected staff member is assessed for any physical safety risk arising from the compromise.
7. Consortium partners (DefendDefenders, Magamba) and relevant civil society security organisations (Access Now Digital Security Helpline) are notified.
8. The incident is logged in the Digital Security Incident Register. Post-incident review within 14 days.

13. Acceptable Use of RFLD Digital Systems

13.1 Permitted Uses

RFLD's digital systems — devices, email, internet access, collaboration tools — are provided for RFLD's programme and operational work. Limited personal use is acceptable where it does not interfere with work duties, does not create security risks, and does not involve:

- Accessing, downloading, or storing any material that violates RFLD's Code of Conduct (RFLD-COC-v1.0).
- Using RFLD systems for any personal commercial activity.
- Installing personal software on RFLD devices.
- Storing significant volumes of personal files on RFLD systems.

13.2 Prohibited Uses

#	Prohibited Activity
1	Accessing, downloading, distributing, or storing sexually explicit, abusive, or illegal content on any RFLD device or system.
2	Accessing, producing, or distributing any content involving child sexual abuse material (CSAM) — zero-tolerance violation; mandatory referral to law enforcement.
3	Using RFLD systems to conduct personal business, commercial activity, or secondary employment.
4	Using RFLD devices or internet access to access gambling, gaming, or entertainment platforms in a way that interferes with work.
5	Accessing social media for personal use in excess of brief, non-disruptive use during working hours.
6	Attempting to access systems, accounts, or data beyond the user's authorised access level — including attempting to access another staff member's email or files.
7	Installing, testing, or deploying any tool that could disrupt RFLD systems or be used for hacking, port scanning, or network reconnaissance — unless specifically authorised by the IT Lead for security testing purposes.
8	Disabling, circumventing, or attempting to disable any RFLD security control — including anti-malware, MDM, or device encryption.
9	Using RFLD systems or data for personal political campaigning or advocacy.

14. Website, Social Media, and External Digital Presence

14.1 RFLD Website Security

RFLD's website (rflgd.org) is a public-facing asset and a potential attack vector. The IT Lead is responsible for website security, applying the following standards:

- HTTPS enforced for all pages — no HTTP access permitted.
- Content Management System (CMS) software, plugins, and themes kept current — updates applied within 14 days of release; critical security patches within 48 hours.
- Web Application Firewall (WAF) active.
- Regular security scanning — monthly automated vulnerability scan; annual manual penetration test.
- Minimal personal data collected via the website — contact forms, newsletter signups, and any data collection subject to DPO review and appropriate privacy notices.

14.2 Social Media Account Security

RFLD's institutional social media accounts (Twitter/X, Facebook/Meta, LinkedIn, Instagram, YouTube, and any others) must be protected with:

- Unique strong passwords stored in the RFLD password manager — not known individually by staff members.
- MFA enabled on all accounts.
- Account access limited to designated Communications staff and the Communications Lead — via the shared vault, not via shared passwords.
- Recovery options (backup email, phone number) registered to RFLD institutional accounts, not personal staff accounts.

All social media posts on RFLD institutional accounts must comply with the Communications standards in the Code of Conduct (RFLD-COC-v1.0 Section 4.9). Any suspected account compromise — unexpected posts, locked account, unusual notifications — is reported to the IT Lead and Communications Lead immediately.

14.3 Staff Personal Social Media

RFLD staff maintain personal social media accounts independently. This Policy does not govern personal accounts except where: the post could be associated with RFLD; the post discloses RFLD programme information; or the account is used in connection with RFLD work. In those cases, the Code of Conduct (Section 4.9) and Communications Policy standards apply. Staff are reminded that their personal social media presence can expose location and activity information useful for targeted surveillance in high-risk contexts — a personal security awareness issue addressed in Section 16.

15. Incident Response Framework

15.1 What Constitutes a Digital Security Incident

A digital security incident is any event — actual or suspected — that has compromised or could compromise the confidentiality, integrity, or availability of RFLD's data or systems. This includes:

- Confirmed or suspected device compromise, including spyware infection.
- Loss or theft of a device containing RFLD data.
- Unauthorised access to RFLD accounts, systems, or data — including successful phishing.
- Ransomware or destructive malware attack on any RFLD system.
- Accidental disclosure of Class 3 or Class 4 data.
- Data breach — any confirmed or suspected exposure of personal data.
- Denial-of-service attack affecting RFLD systems.
- Government seizure or compelled access to RFLD devices or accounts.
- Any other event that causes or could cause harm to RFLD, its data subjects, or the people whose safety depends on RFLD's data security.

15.2 Reporting Obligation — All Staff

Every RFLD staff member who becomes aware of an actual or suspected digital security incident has an immediate obligation to report it to the IT Lead and DPO. Reporting must not be delayed while the staff member tries to investigate or fix the issue themselves. Early reporting gives RFLD the best chance to contain the incident and minimise harm. A staff member who reports a digital security incident promptly, even if they contributed to it, will not be penalised for the reporting. A staff member who conceals or delays reporting will face disciplinary consequences.

15.3 Incident Response Process

Phase	Name	Actions and Responsibilities
1	Detect & Report	Incident identified by any staff member. Report immediately to IT Lead and DPO via phone or Signal. Complete the Digital Security Incident Report Form (Annex C) within 4 hours.
2	Contain	IT Lead takes immediate containment actions — isolating compromised systems; revoking access credentials; activating remote wipe where appropriate; preserving evidence before remediation. DPO activates data breach response if personal data is involved.
3	Assess	IT Lead and DPO assess: What was compromised? What data is at risk? Who is affected? What is the potential harm? Is this a personal data breach requiring notification? Is this a Critical risk requiring Board notification?
4	Notify	Executive Director notified within 4 hours of all incidents involving Class 3 or Class 4 data. Board Chair notified within 24 hours of Critical incidents (device compromise by state actor; Class 4 data breach; ransomware). Sida and relevant donors notified where required by grant agreements.
5	Investigate	IT Lead conducts forensic investigation to determine: root cause; full scope of compromise; data exfiltrated or exposed; persons affected. External specialist engaged if required. Evidence preserved throughout.
6	Remediate	Compromised systems cleaned or rebuilt. Access credentials rotated. Controls strengthened to prevent recurrence. Affected data subjects notified where required by RFLD-POL-DPP-v1.0 and applicable law.
7	Review	Post-incident review within 14 days: What happened? Why? What can be improved? Findings documented. Risk Register updated. Policy or control changes implemented. Lessons shared with staff.

15.4 Notification Timelines

Notification Recipient	Trigger	Timeline
IT Lead + DPO	Any incident detected	Within 1 hour of detection
Executive Director	Class 3 or Class 4 data involved; or any suspected spyware compromise	Within 4 hours of detection
Board Chair	Critical incident (state actor compromise; Class 4 breach; ransomware)	Within 24 hours
Affected data subjects	Personal data breach likely to result in high risk to individuals	Without undue delay — within 72 hours where legally required
National Data Protection Authority	Personal data breach as required by applicable law in relevant country	Per country-specific legal deadline
Sida / GIZ/BMZ / other donors	Incident affecting grant programme activities or requiring donor notification per grant agreement	Per grant agreement timeline — typically within 30 days; immediately for programme-threatening events

16. Security Awareness Training

16.1 Training Requirements

Who	Training Content	Frequency and Deadline
All new staff and consultants	Induction: device security basics; password manager setup; MFA activation; approved tools; classification system; how to report an incident.	Within 5 business days of start — mandatory before accessing Class 3 or Class 4 systems.
All staff — annual refresher	Policy updates; emerging threats; phishing simulation debrief; lessons from actual incidents (anonymised); tool updates.	Annually by 28 February.
helpline and programme staff	Advanced: spyware threat landscape; Lockdown Mode; clean device management; WHRD data handling; board-crossing protocol.	Upon assignment; annually thereafter.
IT Lead and DPO	Advanced: incident response; forensic preservation; threat intelligence; compliance updates.	Quarterly professional development; annual external training.
Board members	Governance-level: RFLD's digital threat context; Board obligations in a data breach; oversight of digital security posture.	Annually at Board development session.
Implementing partners (Tier 3+)	Partner induction: approved tool requirements; incident reporting; data handling obligations under sub-grant agreements.	At partnership inception; annually for multi-year partners.

16.2 Phishing Simulations

The IT Lead conducts unannounced phishing simulations at least quarterly — sending simulated phishing emails to staff to assess click and credential-entry rates. Results are used to: identify individuals who need additional support (not to penalise them publicly); improve training content based on real failure modes; and track improvement over time. The results of phishing simulations are never used as disciplinary evidence.

17. Roles and Responsibilities

Role	Digital Security Responsibilities	Key Deliverables
Executive Director	Accountable to the Board for RFLD's digital security posture; approves policy; receives incident notifications; signs off on Class 4 infrastructure decisions.	Annual security report to Board; Critical incident notifications within 24 hours.
Data Protection Officer (DPO)	Owns this Policy; classifies and governs Class 3 and Class 4 data; reviews all data collection plans; manages personal data breach response; approves access to Class 4 systems.	Annual policy review; data breach notifications; Class 4 access approvals; DPA reviews.
IT Lead	Manages RFLD's technical infrastructure; maintains device registry; enforces security controls; conducts audits; manages incident response; maintains approved tool list.	Quarterly device audits; annual penetration test; Device Register; Incident Register; Approved Tool List (Annex B).
All Staff	Apply classification to information they create or handle; follow approved tool and device standards; use password manager and MFA; report incidents immediately; complete mandatory training.	Training completion; device compliance; incident reporting.
Finance Manager	Applies financial system security controls; ensures financial system MFA is active; manages financial system access rights for departing staff; participates in incident response for financial system incidents.	Financial system access review quarterly; MFA compliance; incident co-response.

18. Partner and Third-Party Digital Security

18.1 Partner Digital Security Requirements

RFLD's programme impact is only as secure as the weakest link in its programme chain. A partner organisation that handles RFLD-provided Class 3 data without adequate security controls is a significant risk — to itself, to RFLD, and to the programme participants whose data it holds. RFLD applies a tiered approach to partner digital security requirements, consistent with partner tier and the sensitivity of the data they handle:

Partner Tier	Data Handled	Required Digital Security Standards
Tier 1 — WAFF Fund	Class 1 and 2 only	No specific digital security requirements beyond Code of Conduct. Basic awareness guidance provided.
Tier 2	Class 2 and limited Class 3	Approved communication channels; secure email for programme data; MFA on shared RFLD platforms; incident reporting obligation.
Tier 3	Class 3 programme data	Approved tool compliance; data classification awareness training; secure file sharing; incident reporting within 24 hours; annual digital security orientation.
Tier 4 — Strategic	Class 3 and Class 4	Full digital security assessment at due diligence; spyware awareness; approved E2EE communications; no commercial cloud for programme data; incident reporting within 4 hours; annual joint security review with RFLD IT Lead.

18.2 Third-Party Service Providers

All third-party service providers with access to RFLD's systems or Class 3/Class 4 data are subject to a Data Processing Agreement (DPA) and a security assessment under RFLD-POL-DPP-v1.0. Access is granted on a least-privilege basis and is reviewed annually. Access is revoked immediately when the service relationship ends.

19. Compliance, Audit, and Enforcement

19.1 Compliance Monitoring

The IT Lead conducts quarterly device compliance audits using the Device Security Checklist (Annex A), verifying that all RFLD devices meet the standards in Section 4. Compliance results are reported to the DPO and Executive Director. Non-compliant devices are remediated within 5 business days or withdrawn from service until compliant.

The DPO conducts an annual information security audit reviewing: data classification compliance; access control appropriateness; incident register analysis; training completion rates; and Class 4 data storage compliance. The annual audit report is presented to the Executive Director and Board Finance Committee.

19.2 Consequences of Non-Compliance

Non-Compliance Type	Examples	Consequence
Minor / inadvertent	Delayed patch application; missed training deadline; brief use of unapproved tool.	Remediation required within 5 days. Documented. Recurring minor non-compliance treated as moderate.
Moderate	Persistent unapproved tool use; failure to apply MFA; repeated late patching; Class 3 data stored in personal cloud.	Formal written notice. Mandatory additional training. Access suspended until controls in place.
Serious	Disabling security controls; sharing credentials; storing Class 4 data on prohibited systems; concealing a security incident.	Disciplinary action under HR Policy. Access suspended. Executive Director involvement. Possible data breach investigation.
Gross Misconduct	Deliberate circumvention of security controls; sharing RFLD data with an unauthorised party; deliberately concealing a device compromise.	Summary dismissal. Referral to law enforcement where evidence supports. Donor notification where required.

20. Governance and Policy Review

20.1 Governance

This Policy is owned by the DPO and maintained operationally by the IT Lead. The Executive Director is accountable to the Board for RFLD's digital security posture. The Board receives an annual digital security report covering: incident summary; training completion; audit findings; key threat developments; and policy or infrastructure changes made or recommended.

20.2 Policy Review Schedule

This Policy is reviewed annually by the DPO and IT Lead, with Board approval. An out-of-cycle review is triggered by: a significant security incident; a major change in the threat landscape (new spyware capability; new zero-day affecting RFLD tools); a new major programme with distinct digital security requirements; or a change in applicable law or standards. The approved tool list (Annex B) is reviewed quarterly by the IT Lead — more frequently than the full Policy, given the pace of change in this area.

20.3 Version History

Version	Date	Summary	Approved By
1.0	May 2026	Initial adoption — RFLD's first standalone Digital Security and Information Management Policy. Covers: four-level information classification system; endpoint security standards; password management with mandatory password manager and MFA; approved/prohibited communications tools matrix; sovereign data infrastructure (DONUESÈ); spyware threat framework including Lockdown Mode and MVT auditing; seven-phase incident response protocol; clean travel device programme; partner digital security tiering. Aligned to RFLD-POL-DPP-v1.0, RFLD-POL-RISK-v1.0, and programme security requirements.	Board of Directors

Policy Approval

Data Protection Officer	IT Lead	Executive Director — Gloria Sekonou
Name:	Name:	Name:
Title:	Title:	Title:
Signature:	Signature:	Signature:
Date:	Date:	Date:

KEY DIGITAL SECURITY CONTACTS — REPORT AN INCIDENT IMMEDIATELY

IT Lead (device issues, malware, access problems): admin@rflgd.org — subject: 'DIGITAL SECURITY INCIDENT — URGENT' Data Protection Officer (data breaches, Class 4 queries): dpo@rflgd.org Executive Director: agueh.dossi@rflgd.org Digital Security Helpline (for WHRDs and activists): rflgd.org/rfld-internal-policies/ Access Now Digital Security Helpline (external support): accessnow.org/help IF YOUR DEVICE MAY BE COMPROMISED: Stop using it. Keep it on. Call the IT Lead immediately.

Annex A — Device Security Checklist

INSTRUCTIONS

Completed by IT Lead for every RFLD-issued device quarterly. Also completed by staff for personal devices used for RFLD work, verified by IT Lead. Non-compliant items must be remediated within 5 business days.

Device Type (Laptop / Phone / Tablet)		Device Serial Number	
Assigned User		Audit Date	
RFLD-Issued or Personal Device		IT Lead Name	

#	Security Control	Compliant	Non-Compliant	N/A
1	Operating system is current and on a supported version	☐	☐	☐
2	All critical and high-severity security patches applied within 14 days of release	☐	☐	☐
3	Auto-update enabled for OS and all RFLD-approved applications	☐	☐	☐
4	Full-disk encryption is active and verified (BitLocker / FileVault / device encryption)	☐	☐	☐
5	Screen lock active with maximum 5-minute inactivity timeout	☐	☐	☐
6	Screen lock requires PIN, passphrase, or biometric — not swipe pattern	☐	☐	☐
7	RFLD-approved anti-malware installed with real-time protection and current definitions	☐	☐	☐
8	Device enrolled in RFLD MDM system (RFLD-issued devices)	☐	☐	☐
9	Only IT-Lead-approved applications installed	☐	☐	☐
10	Device is not jailbroken or rooted	☐	☐	☐
11	No personal USB drives connected to this device	☐	☐	☐
12	RFLD approved VPN installed and configured with kill switch enabled	☐	☐	☐
13	Password manager installed and linked to RFLD account	☐	☐	☐
14	MFA configured for all RFLD system accounts on this device	☐	☐	☐
15	Lockdown Mode enabled (required for high-risk staff: helpline, DPO, ED)	☐	☐	☐
16	Class 4 data not stored locally on this device	☐	☐	☐

Non-compliant items and remediation plan (with target date):

IT Lead — Signature & Date	Device User Acknowledgement — Signature & Date
Name:	Name:
Title:	Title:

Signature:	Signature:
Date:	Date:

Annex B — Approved Tools Reference List

INSTRUCTIONS

Maintained by IT Lead. Reviewed quarterly — tools added or removed as the security landscape changes. Staff must not use tools not on this list for RFLD work. Request tool additions via IT Lead assessment.

Category	Approved Tool(s)	Max Classification	Notes
Encrypted messaging	Signal	Class 4 (with disappearing messages for Class 4)	Required for Class 3 and Class 4. Disappearing messages mandatory for Class 4.
Encrypted messaging (alternative)	Wire / Element	Class 3	Where Signal is not available. DPO approval for Class 4.
RFLD email	[RFLD-hosted email system]	Class 2 (Class 3 with S/MIME)	S/MIME required for Class 3 email. Class 4 never via email.
VPN	[RFLD-approved VPN client]	All classifications	Mandatory outside RFLD offices. Kill switch must be enabled.
Password Manager	[RFLD-approved password manager]	All classifications	All RFLD accounts must be managed via the password manager.
MFA Authenticator	Aegis (Android); Microsoft Authenticator; Authy	All accounts	TOTP apps preferred over SMS-based MFA.
Hardware Security Key	FIDO2/WebAuthn-compatible key (Yubico or equivalent)	Class 4 system access	Required for DONÜESÈ and helpline system access.
Anti-malware	[RFLD IT Lead-specified]	All devices	Managed by IT Lead; auto-update required.
File storage — Class 2	[RFLD-approved cloud storage]	Class 2	Access-controlled; not personal cloud.
File storage — Class 3	[RFLD-managed encrypted storage]	Class 3	Access-controlled; TLS + encryption at rest.
File storage — Class 4	RFLD DONÜESÈ Data Center exclusively	Class 4	No alternatives permitted.
Link checking	VirusTotal or equivalent	N/A (tool for checking URLs)	Use for suspicious links before clicking.
Video conferencing	[IT Lead-approved platform]	Class 2 only	No Class 3 or Class 4 content in video calls on commercial platforms.

Note: Specific tool names (VPN, email system, file storage) are specified in RFLD's internal IT configuration document, maintained by the IT Lead and updated as tools are changed. This Annex reflects the category and classification limits — Annex B is valid even when specific tool names change, provided the category and classification requirements remain consistent with this Policy.

Annex C — Digital Security Incident Report Form

INSTRUCTIONS

Complete within 4 hours of detecting any digital security incident. Submit to IT Lead and DPO simultaneously. For Critical incidents (state actor compromise; Class 4 data breach), call the IT Lead immediately before completing the form.

Reporting Person		Report Date and Time	
Incident Discovery Date/Time		Location (Office / Country)	
System(s) / Device(s) Affected		IT Lead Notified? (Date/Time)	
Incident Category (tick all that apply)	☐ Device lost/stolen ☐ Suspected spyware/malware ☐ Phishing / credential compromise ☐ Ransomware ☐ Unauthorised access ☐ Data breach / accidental disclosure ☐ Government device seizure ☐ Other: _____		
Data Classification of Affected Data	☐ Class 1 — Public ☐ Class 2 — Internal ☐ Class 3 — Confidential ☐ Class 4 — HIGH RISK ☐ Unknown		

Describe what happened — as specifically as you can, including any unusual device behaviour, messages received, or actions you took before discovering the incident:

What data do you believe may have been compromised, accessed, or exposed?

Who else may be affected — other staff, programme participants, partners, or beneficiaries?

What immediate actions have you taken so far (e.g., stopped using device, changed passwords)?

Has the affected device been isolated from RFLD networks? (Yes / No / Unknown)

Do you believe this could be a state-sponsored or targeted attack? (Yes / No / Unknown — explain):

IMPORTANT: Do not attempt to remediate, clean, or factory-reset any device involved in a potential spyware compromise before the IT Lead has conducted forensic assessment. Remediation before forensic capture destroys evidence.

Reporter — Signature & Date	IT Lead Received — Signature, Date & Time

Annex D — Digital Security Quick Reference Card

PRINT THIS CARD. Keep it accessible — in your wallet, on your desk, or as a phone wallpaper. This is what every RFLD staff member must know and do.

Your Daily Digital Security Habits

	Do This Every Day
✓	Lock your screen when you leave your device — even for 2 minutes.
✓	Activate VPN before accessing any RFLD system outside the office.
✓	Never click a link or open an attachment in an unexpected email — report it to the IT Lead.
✓	Use Signal (not WhatsApp) for any programme-related message involving partner or beneficiary information.
✓	Never store Class 4 data locally on your device — it belongs on the DCONUESÈ Data Center only.
✓	If your device behaves unusually — battery draining fast, running hot, unexpected notifications — stop and call the IT Lead.

Information Classification — What You Need to Know

Class	Label	Key Rule
1	PUBLIC	Share freely. Use any channel.
2	INTERNAL	RFLD systems only. No personal accounts.
3	CONFIDENTIAL	Encrypted channels only. Need-to-know access. Password-protect files.
4	HIGH RISK	Signal only. DCONUESÈ only. No email. No cloud. Report any uncertainty to the DPO immediately.

If You Think Something Has Gone Wrong — Contact These People Immediately

Suspicious email / phishing attempt	IT Lead — admin@rflgd.org — 'DIGITAL SECURITY — PHISHING'
Lost or stolen device	IT Lead FIRST — then DPO. Within 2 hours.
Suspected device compromise / spyware	Stop using the device. Call IT Lead immediately. Do not factory-reset.
Data breach / accidental disclosure	DPO — dpo@rflgd.org — immediately.
Government seizure of device at border	IT Lead + DPO as soon as safely possible. Complete Annex C.
Any doubt about classification or handling	DPO — dpo@rflgd.org — ask before acting, not after.

When in doubt — STOP and ASK. dpo@rflgd.org | admin@rflgd.org

