



GUIDANCE FOR USING A BRING YOUR OWN DEVICE (BYOD) STRATEGY IN INSECTICIDE-TREATED NET (ITN) CAMPAIGN DIGITALIZATION

JULY 2026



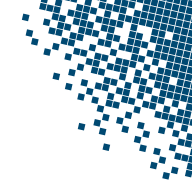
CONTENTS

Glossary	4
1. Background	5
1.1 What is BYOD in ITN campaigns?	5
1.2 Planning for BYOD	6
1.3 Device strategy models	7
1.4 Benefits and risks	8
1.5 Considerations for choosing a device strategy	9
2. Scope and use cases for BYOD in ITN campaigns	11
2.1 When BYOD is appropriate or not appropriate	11
2.2 Assessing BYOD feasibility and readiness	13
3. Policy, privacy and security	22
3.1 Developing the BYOD policy	22
3.2 Define acceptable use and responsibilities	22
3.3 Set minimum security and access controls	23
3.4 Establish data governance and storage rules	23
3.5 Incident response for lost, shared or compromised devices	24
4. Implementation of BYOD	25
4.1 Fallback arrangements	25
4.2 Training	25
4.3 Support and supervision during implementation	26
4.4 Daily operational controls	26
4.5 Post-campaign device closeout	27
5. Conclusion	28
Annex 1: BYOD readiness assessment checklist	29
Annex 2: BYOD enrolment, device verification and consent form	32
Annex 3: Device inventory template	35
Annex 4: Sample BYOD policy and terms of use for ITN campaigns	36



GLOSSARY

Term	Definition
API	Application Programming Interface (Android interface between the app and the server). It identifies which functions and features are available in a specific version of the operating system.
Bring Your Own Device (BYOD)	A policy that allows individuals to use their personal devices for approved campaign tasks under defined governance, consent and support arrangements.
Campaign applications (apps)	Approved digital tools used for ITN campaign tasks, such as household registration, distribution recording, supervision checklists or stock management.
Data protection impact assessment (DPIA)	A process used to identify and minimize data protection risks associated with a project, system or data processing activity.
GPS	Global Positioning System
Hybrid BYOD	A model in which campaign implementation uses a mix of personal devices and programme-owned devices.
Mobile Device Management (MDM)	Software that enables a programme to manage, monitor and remotely control aspects of devices enrolled for campaign use. In BYOD contexts, this is usually limited to app-level controls.
Offline-first	An application architecture in which core functions and data entry operate without an active internet connection, with data synchronized when connectivity becomes available.
Programme-owned device (POD)	A device purchased and owned by the programme/other Ministry of Health or government entity or implementing partner, configured and issued to workers for campaign use.
Pure BYOD	A model in which campaign workers use their own phones and SIM cards across selected digitalized campaign phases and functions.
Remote wipe	The ability to delete campaign data from a device remotely.
Rooting (Android) and jailbreaking (iOS)	Processes that remove manufacturer or carrier restrictions, granting users “root” or administrator-level access to the operating system.
Role-based access	A security approach in which users can access only the data and functions relevant to their assigned role(s).
Synchronization (sync)	The process of transferring locally stored data from a device to a central server.
Zero-rated data	Mobile data access for a specific application that does not consume the user’s personal data allowance.



1. BACKGROUND

Malaria remains a significant public health challenge in many endemic countries. Insecticide-treated nets (ITNs) continue to be one of the most effective interventions for reducing malaria transmission and preventing morbidity and mortality. In most malaria-endemic countries, ITN mass distribution campaigns are commonly implemented at scale and within compressed timelines to rapidly increase household access to ITNs and community-level protection against malaria.

The operational demands of these campaigns require timely, accurate and complete data. Tight implementation schedules, large numbers of temporary workers and complex last-

mile logistics all depend on reliable information to support planning, supervision and corrective action. Data quality and timeliness are therefore critical to campaign performance.

Digitalization of selected campaign functions can address many of these challenges. However, procuring and managing large quantities of standardized mobile devices is costly, time-consuming and operationally demanding. In many settings, these constraints may limit the feasibility or scalability of fully digitalized campaigns. One practical alternative is the use of personally owned mobile devices by campaign workers, commonly referred to as Bring Your Own Device (BYOD).

1.1 What is BYOD in ITN campaigns?

BYOD is a strategy that allows campaign workers to use their personal devices, typically smartphones, for approved campaign tasks. Under BYOD, vetted (see below) personal devices are temporarily enrolled to run approved campaign applications. Campaign workers access tools and data collection apps on devices they already own and know how to use.

This approach is particularly valuable where campaign budgets make it operationally challenging to procure and manage large quantities of programme-owned devices. Beyond financial savings, BYOD has been shown to boost productivity and user satisfaction, as field staff can perform work tasks on familiar devices with which they are comfortable¹.

Several countries have applied BYOD in ITN campaigns. Uganda presented its experience using BYOD for the digitalization of ITN universal

coverage campaigns at the 2023 AMP Campaign Digitalization Meeting². Togo documented the use of personal devices in its 2020 and 2023 mass ITN campaigns in a case study published on the AMP website³. These experiences indicate that BYOD can be operationally feasible in campaign settings when supported by clear eligibility criteria, a comprehensive strategy for use, data support arrangements and a loaner device pool for workers who do not own a compatible smartphone or do not wish to use their own.

This guide provides practical recommendations and operational considerations for BYOD in ITN mass distribution campaigns. It is intended for national malaria programmes (NMPs), their implementing and financing partners, and digital health providers supporting the planning and delivery of ITN campaigns.

1. <https://www.tandfonline.com/doi/full/10.1080/08874417.2018.1543001>

2. https://allianceformalariaprevention.com/wp-content/uploads/2024/02/2.8-Rukaari-Medard_Uganda.pdf

3. <https://allianceformalariaprevention.com/resource-library/resource/digitalization-of-the-2020-and-2023-mass-itn-campaigns-in-togo-the-experience-of-bring-your-own-device-byod/>



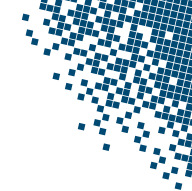
The following recommendations summarize the main actions for safe and effective implementation of a BYOD strategy and are further discussed in the guidance:

- **Establish a BYOD strategy before any enrolment begins.** Define acceptable use, user responsibilities, data protection requirements, security standards, compensation, incident reporting and liability. Obtain Ministry of Health/national malaria programme (MoH/NMP) leadership endorsement and complete legal review.
- **Define and enforce minimum device and security standards.** Verify every device during enrolment. Do not enrol devices that do not meet requirements.
- **Provide differentiated, practical training adapted to the digital literacy of each user group.** Verify competency before deployment. Ensure technical support is accessible throughout implementation.
- **Apply proportionate security controls.** At minimum: secure login, role-based access, encrypted storage, session timeout and remote logout capability. Apply stronger controls for higher sensitivity workflows.
- **Use a hybrid approach.** BYOD is not suitable for all campaign functions or all users. Reserve programme-owned devices for high-risk workflows. Maintain a loaner pool and a tested paper fallback or alternative solution.
- **Ensure BYOD does not create unfair costs for workers.** Define data bundle support and compensation arrangements before the campaign begins and communicate them clearly at training.
- **Monitor implementation using defined indicators from the pilot stage onward.** Adjust scope, safeguards, or deployment model based on evidence. Do not scale up an approach that is not meeting pilot objectives.

1.2 Planning for BYOD

BYOD should be planned early to ensure that it will be appropriate and the required results achieved. Planning requires NMPs to complete the following steps in sequence, for which further details are given in the later sections of the guidance:

1. **Conduct a BYOD feasibility assessment and document the decisions:** This should confirm whether BYOD is appropriate, where it can be used and which approach should be used ([Section 2.2](#)).
2. **Define the minimum device requirements for campaign use:** These should reflect the needs of the campaign application and the minimum security standards required ([Section 2.2.1](#)).
3. **Conduct the device census and classify users by readiness tier:** This helps determine how many workers have suitable devices, where gaps exist, and the likely size of a loaner device pool for those without their own ([2.2.1](#)).
4. **Confirm and test that the selected platform is suitable for BYOD:** The platform should work on the types of personal devices expected in the campaign, especially common Android phones. Testing should include a representative sample of real devices, including low-end models, and should confirm offline functionality, synchronization performance and usability in the target areas ([2.2.4](#)).



- 5. Draft and validate the BYOD policy and related user forms:** This includes user acknowledgement or consent forms in the main local languages, as required (Section 3, and Annexes 2 and 4).
- 6. Calculate budget requirements and secure approval:** BYOD reduces device procurement costs but other operational costs remain regardless of whether programme-owned devices or personal devices are used and must therefore be budgeted prior to roll-out. Costs may include data bundle support, airtime, loaner devices, SIM cards, power banks, training and technical support (2.2.6).
- 7. Procure and configure the loaner device pool and other required support items:** This should be done early enough to support enrolment, allow alternative arrangements and ensure full worker inclusion.
- 8. Run a pilot in representative districts and review the results before roll-out:** The pilot should test the approach under realistic conditions and assess performance against the agreed scale-up criteria. Where performance against agreed criteria is not met, scope, safeguards or deployment model should be revised before roll-out (2.2.8).

1.3 Device strategy models

ITN campaigns may use different device strategies depending on the context. While some settings may be suitable for pure BYOD or full programme-owned device (POD) deployment,

most campaigns are likely to benefit from a hybrid approach that combines personal devices with a targeted pool of programme-procured devices (Table 1).

Table 1: Device strategy models for ITN campaign digitalization

BYOD model	Description	Best suited for
Pure BYOD	Campaign workers use their own phones and SIM cards across selected digitalized campaign phases and functions.	Contexts with high smartphone penetration, established implementer networks, reliable connectivity and lower requirements for device standardization and control.
POD	A standardized device is procured, configured and issued to every campaign worker needing to use the digital tool. All devices are programme-owned and managed throughout their lifecycle, including distribution, reverse logistics, storage and maintenance between campaigns.	Campaigns where smartphone ownership among target campaign workers is low, where national data protection requirements restrict personal device use, where all campaign functions require full device-level security controls, or where it is planned to reuse devices across multiple campaign cycles and interventions.
Hybrid BYOD	Campaign implementation uses a mix of personal devices and programme-procured devices. Programme-procured devices are allocated where smartphone ownership is low or where greater standardization, reliability or security is required.	Most campaigns. Best suited for programmes seeking the cost and familiarity benefits of BYOD while reducing implementation risk and ensuring coverage for workers or functions that cannot rely on personal devices alone.



NMPs using BYOD should plan for a small loaner device pool, for example around 5–10% of the intended BYOD workforce, to support inclusion and operational continuity for workers whose devices do not meet minimum requirements or who choose not to use their personal device

for campaign work. Where feasible, this loaner pool can be supplemented through coordination with other health programmes and partners to temporarily borrow or reallocate existing devices.

1.4 Benefits and risks

BYOD can offer important operational and cost advantages, but only when it is appropriate to the context and when associated risks are actively managed. The balance between benefits and risks will vary by campaign setting, so programme managers should assess both before deciding whether and how to use BYOD.

Potential benefits include:

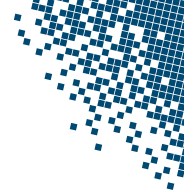
- Reduced costs for device procurement, storage and distribution.
- Faster deployment, with no need for large-scale device procurement and configuration.
- Workers use familiar devices, which may reduce the learning curve and training time.
- Enables rapid scale-up without complex device logistics.
- Personal ownership may encourage greater care in device handling and use.
- Exposure to campaign applications can build digital familiarity for future health programme use.
- Avoids post-campaign device collection, storage, maintenance and e-waste burden.
- Training materials and job aids can be pre-loaded on workers' devices, with updates and refresher guidance easily shared during implementation as needed. This may include short training reminders or troubleshooting prompts when issues arise, all of which can be delivered through lightweight channels such as links to YouTube or other commonly used digital platforms.

- May reduce programme spending on replacement devices and accessories in some settings.

The benefits must, however, be weighed up with potential risks which may include:

- Variation in device quality and compatibility with the campaign application.
- Equity concerns, including gender and broader digital divide issues, where some workers do not own suitable smartphones or have equal access to digital tools.
- Data protection risks when personal and campaign data coexist on the same device.
- Unclear liability if a personal device is lost, damaged or compromised.
- Connectivity limitations and failures in offline synchronization.
- Increased support needs and possible data quality issues where digital literacy is limited.
- Risk of unauthorized access if devices are shared or inadequately secured.
- Disputes over incentives or reimbursement if arrangements are not clearly defined.
- Variation in operating systems and device settings may complicate technical support.

Further risks and measures for their mitigation can be found in [Section 2.2.9](#).



1.5 Considerations for choosing a device strategy

Before committing to a single device strategy, malaria programme managers and supporting data/M&E and ICT personnel should assess how pure BYOD, full POD and hybrid BYOD compare across the key operational and policy dimensions relevant to their campaign. As noted

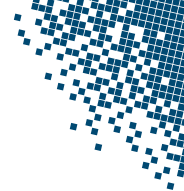
in Table 1, the hybrid BYOD model is the recommended default for most campaigns. The framework below (Table 2) is intended to help programme managers confirm or adjust that default based on their specific context.

Table 2: Decision framework for selecting a device strategy

Decision dimension	Favours BYOD	Favours full POD	Hybrid BYOD
Upfront cost	Lower since device procurement is expensive and there is often limited time to procure devices.	Lower over time when devices will be reused across multiple campaign cycles and interventions.	Reduces total procurement cost by limiting programme purchase to a defined subset of devices that should be planned for reuse across different interventions and activities.
Procurement lead time	Fastest: no procurement process required for personal devices.	Requires lead time for procurement, configuration and distribution of all devices.	Shorter than full POD, as fewer devices need to be procured and configured. Programmes should still allow time for loaner pool procurement.
Device availability	Only viable if smartphone penetration is sufficiently high among target worker cadres across all campaign zones.	Ensures every enrolled worker has a compatible device regardless of personal ownership.	Broadens coverage by using personal devices where ownership is high, and allocating programme-procured devices to cadres, zones or roles where smartphone ownership is low or device standardization is required.



Decision dimension	Favours BYOD	Favours full POD	Hybrid BYOD
Worker familiarity	Workers know their own devices; faster user adoption and fewer device-related errors during routine tasks.	Requires additional training time on an unfamiliar device and operating system.	Retains the familiarity benefit for workers using personal devices while providing standardized devices and training for selected roles and geographies.
Data security control	Limited: the programme cannot fully control a personal device. App-level controls are the most feasible approach.	Allows full Mobile Device Management (MDM), encryption and device configuration under programme control.	Applies full device-level controls to programme-procured devices used for higher-risk workflows such as payments and system administration. Personal devices used for other functions operate under app-level controls.
Loss and damage liability	Ambiguous unless the BYOD policy defines liability clearly before enrolment.	Programme bears the full cost of loss and damage for all devices.	Liability follows device ownership. Programme-procured devices are covered by the programme; personal devices are governed by the terms defined in the BYOD policy.
Post-campaign management	No device reverse logistics but remote app removal and data deletion required and should be verified.	All devices should be collected after each campaign, securely stored, maintained, and reused for subsequent campaigns where applicable.	Easier than full POD, as only programme-owned devices require retrieval, storage and maintenance. Remote app removal and data deletion required for personal devices.



Decision dimension	Favours BYOD	Favours full POD	Hybrid BYOD
Equity and inclusion	Risk of exclusion where some workers, particularly women and older workers, lack compatible smartphones.	Ensures equal access regardless of personal device ownership.	Directly addresses the equity risk by allocating programme-procured devices to workers who do not own a compatible smartphone or who opt out of BYOD.

No single model is appropriate for all campaigns. The choice should be informed by the device census results (Section 2.2.1), the cost analysis (Section 2.2.6), and assessment of workforce readiness, data sensitivity and operational risk. In most settings, the hybrid BYOD model offers the strongest balance of cost efficiency, inclusion and risk management. Pure BYOD may be appropriate where smartphone

ownership is very high and no campaign functions require elevated security controls. A full POD approach should be considered where smartphone ownership among the target workforce is low, where national data protection requirements restrict personal device processing, or where it is planned to reuse devices across multiple campaign cycles or different activities/interventions.

2. SCOPE AND USE CASES FOR BYOD IN ITN CAMPAIGNS

2.1 When BYOD is appropriate or not appropriate

BYOD is not suitable for every campaign, role or location. Its use depends on the operational context, workforce profile, digital system requirements, the programme management's ability to manage risk and alignment with government data policies. The consequences of deploying BYOD in unsuitable conditions extend beyond operational disruption: if data collection fails because devices are incompatible or workers cannot use them effectively, households may go unregistered and families may not receive the ITNs they need.

In most ITN campaigns, BYOD is best suited to lower-risk operational functions such as household registration, distribution recording, supervision and monitoring activities, especially where smartphone access is high and connec-

tivity is adequate. However, BYOD can also be used for activities involving personal or sensitive data, provided that appropriate safeguards are in place to ensure data protection, security and accountability. The key consideration is not whether personal data are involved, but whether sufficient controls can be enforced over how data are accessed, stored and transmitted. Where such controls are harder to guarantee, or where higher levels of assurance and oversight are required, programme-owned devices may be more appropriate.

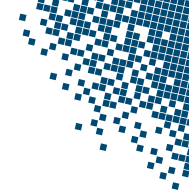
Suitability may also vary by geography. BYOD is generally more feasible in urban and peri-urban areas with reliable internet connectivity, access to charging and widespread smartphone use. In rural, remote or conflict-affected areas with

poor internet coverage, limited charging or low smartphone penetration, programme-owned devices or a hybrid approach may be more appropriate. Where not all defined suitability criteria and conditions can be met, a hybrid model is usually the most practical option.

Before adopting BYOD, programmes should assess whether the minimum technical, policy and implementation conditions are in place. Table 3 provides a simple framework for that assessment.

Table 3: Suitability framework for BYOD adoption

Use BYOD when:	Limit or avoid BYOD when:	Do not use BYOD when:
Smartphone ownership among campaign workers is high enough to cover most required roles.	Access to suitable devices is highly inequitable and many required worker cadres do not have smartphones that meet minimum requirements.	The device does not meet minimum security requirements (rooted, jailbroken, no encryption support, no screen lock).
Workers are already using smartphones for other digital health programmes.	Digital literacy gaps are likely to significantly affect implementation quality and data reliability.	National policy or the Data Protection Authority explicitly prohibit personal device processing for the relevant data category.
Offline functionality and synchronization have been tested and confirmed.	Connectivity and synchronization challenges are likely to compromise data completeness or timeliness.	Tasks require storing or processing bulk financial credentials or banking details; use programme-owned devices for all payment workflows.
Technical support can be provided for a diverse range of devices.	Technical support capacity is too limited to manage device diversity effectively.	The programme cannot provide an opt-out alternative or reasonable compensation for personal device use.
Timelines or budgets make large-scale procurement of programme-owned devices impractical.	Security risks cannot be mitigated to an acceptable level with available resources.	
Minimum security and data protection measures can be enforced consistently.	Highly sensitive data cannot be sufficiently minimized, protected or segregated on personal devices.	
A clear incentive, compensation and accountability framework is in place.	Policy, legal or governance requirements remain unresolved.	



2.2 Assessing BYOD feasibility and readiness

BYOD should not be adopted by default. Before selecting BYOD as a campaign modality, NMPs should assess the device landscape, application readiness, connectivity constraints, legal and data protection requirements, workforce inclusion implications, support capacity and overall implementation risk. Where major gaps are identified, they should be addressed before implementation, or a hybrid or programme-owned device approach should be used instead.

In practice, the assessment should begin during the macroplanning stage, not after the campaign platform has already been selected. [Annex 1](#) provides a BYOD readiness assessment checklist covering the main domains to be reviewed during macroplanning.

2.2.1 Device landscape and minimum device requirements

A BYOD assessment should start with a review of which devices the campaign workforce owns and whether those devices can support the

campaign application. Smartphone ownership alone is not enough. NMPs should use the BYOD enrolment and consent form ([Annex 2](#)) to collect basic information on device type, model, operating system, storage, battery, GPS, camera and screen lock status, and then classify users by zone and role as fully compatible, compatible with conditions or not compatible. [Annex 2, part 2](#) (Device inventory and specification check) is an example of an inventory of users and confirmation of compatibility.

Users who do not meet the minimum requirements should be supported through a loaner device pool or alternative arrangement. Table 4 provides indicative minimum device requirements for BYOD participation, based on common functional requirements observed across digital campaign data collection tools and typical specifications needed to ensure compatibility, usability and data security in field operations. Final thresholds should be confirmed during campaign planning based on the selected application.

Table 4: Example minimum device requirements for BYOD participation

Specification	Minimum requirement	Notes
Operating system	Android 8.0+ (API level 26+) or iOS 13+	Confirm the exact API level with the app developer.
RAM	2 GB	Devices with 1 GB may open the app but are likely to crash under field conditions.
Free internal storage	2 GB minimum before app installation	Should cover app, offline data cache for 2–3 days and media attachments.
Battery performance	Sufficient for a full working day (6–8 hours minimum)	Assess actual battery health, not only original stated capacity.
Screen size	5.0 inches minimum	Smaller screens increase navigation difficulty and data entry errors.
GPS	Required where the app captures location data	Confirm acceptable GPS accuracy threshold, typically within 20 metres.



Specification	Minimum requirement	Notes
Camera	Required where the app uses QR/barcode scanning	Test on common low-end device models in the campaign area.
Encryption	Device supports app-level or full-disk encryption	Full-disk encryption is enabled by default on Android 6.0+ and iOS 8+.
Security	Screen lock enabled	A screen lock is an absolute exclusion criterion if not in place.
Security	Device not rooted or jailbroken	Rooted or jailbroken devices are an absolute exclusion criterion.

2.2.2 Legal, policy and data protection feasibility

Legal and policy feasibility should be reviewed early. If national law, ministry policy or programme rules do not allow the relevant data to be processed on personal devices, BYOD should not be used.

Programme managers should:

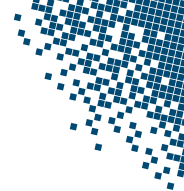
- Review national data protection and health data rules.
- Confirm whether personal-device processing is permitted.
- Identify any data localization or hosting requirements.
- Classify campaign data by sensitivity.
- Complete a data protection impact assessment where higher-risk data are involved.

Where GPS data could create risk, especially in conflict-affected or sensitive settings, programmes should reduce precision, restrict access, avoid household-level location capture or follow other national/sub-national policy where appropriate.

2.2.3 Equity, inclusion and opt-out arrangements

BYOD must not create or reinforce inequities in campaign participation. Readiness should be assessed disaggregated by gender, age group, cadre and geography. In many contexts, women volunteers and older workers have lower smartphone ownership rates and digital literacy.

- Participation in BYOD must be genuinely voluntary; workers must not be penalized for declining to use a personal device.
- A viable alternative must always be available, such as a programme-owned loaner device or a non-BYOD role within the campaign.
- Incentive structures must not be designed in a way that compels participation; BYOD participation should be separated from payment eligibility.
- A loaner device pool covering at least five to ten per cent of the intended BYOD workforce should be budgeted and pre-positioned.



2.2.4 Connectivity, offline readiness and platform suitability

Planning should be based on the weakest expected field conditions, not average network coverage.

- Map connectivity by campaign zone and test synchronization performance in representative low-connectivity areas.
- The application must function fully offline for all essential workflows. Local storage must be sufficient for at least two to three days of submissions without a sync.
- Define sync points (health facilities, schools, district offices) and expected sync cadence, at least daily during active distribution.
- Confirm that duplicate prevention logic functions offline, not only when connected.
- Supervisors must be able to identify which devices have not synchronized within the expected window; this is a mandatory feature for the monitoring dashboard.

The platform should be tested on the types of devices that campaign workers actually own, including low-end Android models common in many settings.

2.2.5 Security and support arrangements

For most ITN campaign contexts, app-level security controls, including encryption, authentication and remote de-authentication, combined with strong operational oversight, are the most feasible approach.

At a minimum:

- Devices that have been modified to bypass standard operating system security controls (rooted Android devices, jailbroken iPhones) should not be permitted.
- Campaign data should not be exported to personal applications. Appropriate technical controls should be implemented to prevent or restrict such exports wherever feasible.
- Devices should have screen lock enabled.
- Access should be role-based.
- User sessions should expire automatically after inactivity.

A heterogeneous fleet of personal devices places higher demands on technical support than a standardized POD fleet. A tiered support structure should be in place before roll-out.

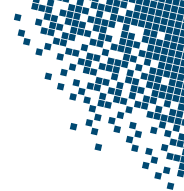
2.2.6 Cost considerations

BYOD may reduce device procurement costs, but it does not remove programme costs. Programmes should compare the full cost of BYOD against the cost of programme-owned devices,

rather than focusing only on phone purchase costs. Table 5 shows cost comparisons between the two approaches.

Table 5: Cost comparison of BYOD and programme-owned devices (POD)

Cost category	BYOD approach	POD approach	Level of resource change (BYOD vs. POD)
Device acquisition	No direct cost to the programme.	Full cost borne by the programme.	Lower
Data bundles/airtime	Stipend, allowance or reimbursement for campaign use.	Programme procures SIM cards and data plans for all devices.	Same
Technical support	Higher, due to variation in device types and configurations.	Lower, as devices are standardized and pre-configured.	Higher
Training	Slightly higher, as device variability increases training needs.	More standardized, as all devices are the same.	Higher
Device loss/damage	Responsibility defined by policy; compensation usually limited.	Full replacement cost borne by the programme.	Lower
Post-campaign recovery	No device collection required; campaign access and data should be removed.	Devices are collected after each campaign, stored, maintained and reused for other campaigns where applicable.	Lower
Device management/licensing	Usually limited to app-level controls, with lower cost.	Full device management may be required, with higher cost.	Lower
Loaner device pool	Usually required for 5–10% of the workforce.	Not usually required but a contingency stock is needed for implementation.	Lower
E-waste management	Not applicable to the programme.	Required at end of device life.	Lower



2.2.7 Reimbursement and compensation

Workers should not bear the cost of campaign digitalization from personal resources. Compensation arrangements should be defined before implementation begins:

- Pre-loaded data bundle SIM cards issued at training.
- A flat daily data allowance or stipulated amount based on work paid alongside other campaign stipends.
- Zero-rated data access for the campaign platform, which requires negotiation with the national telecommunications operator and is feasible in some countries.

2.2.8 Pilot and scale-up decision

BYOD should be piloted before wider roll-out, especially where it is being used for the first time or where connectivity and device quality vary across locations. Pilot sites should reflect the main implementation conditions expected in the campaign. The programme should only be scaled up when the pilot demonstrates that:

- Most enrolled BYOD users can submit valid records.
- Synchronization works within the expected timeframe.
- Data completeness is acceptable.
- Technical issues can be resolved quickly.
- Fallback to paper or programme-owned devices remains limited.

Where pilot results show major gaps, they should be addressed before scaling up or reduce the scope of BYOD.

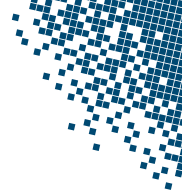
2.2.9 Risk assessment and mitigation plan

The use of personal devices introduces operational, technical and data protection risks that should be identified and managed early. These risks should be assessed during planning and practical mitigation measures put in place before roll-out. Table 6 below summarizes common BYOD risks and suggested mitigation measures.

NOTE: The risks and mitigation table is also reproduced in Excel as an adaptable tool annexed to the document. This tool may be downloaded and adapted by NMPs considering a BYOD strategy to inform their *Risk assessment and mitigation plan*.

Table 6: Key BYOD risk areas, priority and mitigation measures *(also available as an adaptable tool in Excel)*

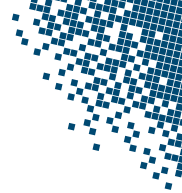
Category	Risk area	Example risk	Mitigation measures
Technical	Device compatibility	Personal devices do not meet minimum app requirements	Define minimum device specifications; conduct device census and verification before roll-out; maintain a loaner device pool
Technical	Device performance	Low battery life, limited storage, app crashes, or poor GPS accuracy	Test app on common device types; require minimum RAM and storage; provide charging guidance or power banks where feasible
Technical	Technical support	Mixed device types create more support needs than expected	Set up tiered support arrangements; prepare troubleshooting guides; train supervisors to resolve basic issues
Technical	Platform stability	App or platform failure disrupts campaign implementation	Test the platform before roll-out; define escalation procedures; maintain vendor support and fallback arrangements
Operational	Connectivity and synchronization	Weak network coverage delays sync and affects real-time monitoring	Use offline-first applications; define sync points and sync schedules; provide supervisor monitoring for non-synced devices; plan paper or POD fallback where needed
Operational	Data quality	Inconsistent digital literacy or unfamiliar workflows lead to incomplete or inaccurate submissions	Provide practical, role-based training; simplify forms; use in-app validation and skip logic; strengthen supervisor review



Category	Risk area	Example risk	Mitigation measures
Operational	Duplication and fraud	Multiple submissions for the same household or unauthorized entries	Use unique identifiers, duplicate checks, audit trails and supervisor review; apply server-side validation where possible
Operational	Incident reporting	Device loss, misuse or technical problems are not reported quickly enough	Establish a clear incident reporting process; train users and supervisors on escalation steps; share support contacts widely
Security	Data protection and privacy	Personal and campaign data coexist on the same device, increasing risk of unauthorized access or sharing	Use secure login, role-based access and encryption; restrict data export; require screen lock; provide clear acceptable use guidance
Security	Device loss or theft	A device containing campaign data is lost, stolen or replaced during implementation	Require immediate incident reporting; enable remote deactivation or data wipe where possible; limit local data storage; verify replacement devices before use
Security	Shared device use	Household members or other users access the campaign app or data on a shared phone	Require individual user accounts; prohibit account sharing; assess whether BYOD is suitable where private device use cannot be assured
Security	Unsafe device configuration	Rooted or jailbroken devices bypass security controls	Exclude rooted or jailbroken devices from BYOD participation; verify device status during enrolment
Security	Post-campaign data residue	Campaign data remain on personal devices after the campaign ends	Apply a closeout process; deactivate accounts; clear local data where required; conduct spot-checks where feasible



Category	Risk area	Example risk	Mitigation measures
Security	Sensitive location data	GPS data expose households in conflict-affected or politically sensitive areas	Reduce GPS precision where needed; restrict export of location data; assess risk by zone before roll-out
Legal/governance	Governance and accountability	Unclear responsibility for device-related incidents, policy violations or non-compliance	Define user responsibilities, incident reporting pathways, and consequences for non-compliance in a simple BYOD policy
Legal/governance	Regulatory compliance	Personal device processing of household data is restricted by national law or authority	Review legal requirements early; conduct a Data Protection Impact Assessment (DPIA) where appropriate; engage relevant authorities; limit collection of personal data to the operational minimum
Legal/governance	High-risk functions	Sensitive activities such as bulk payments or system administration are performed on personal devices	Restrict high-risk functions to programme-owned, controlled devices
Equity/HR	Equity and inclusion	Some workers do not own suitable smartphones or prefer not to use personal devices	Make BYOD voluntary; provide programme-owned or loaner devices; use hybrid deployment where needed
Equity/HR	Coercion or unfair participation pressure	Workers feel compelled to use personal devices to remain eligible for work or payment	Separate BYOD participation from payment eligibility; provide opt-out options; communicate the policy clearly during training
Equity/HR	Policy comprehension	Workers do not fully understand BYOD conditions or responsibilities	Use plain language and local language forms; provide verbal briefing and comprehension checks during training



Category	Risk area	Example risk	Mitigation measures
Financial/ sustainability	Incentives and reimbursement	Workers incur data or charging costs and feel unfairly treated	Define clear compensation arrangements before roll-out; provide data bundles, stipends or other support
Financial/ sustainability	Device replacement expectations	Workers expect the programme to replace damaged or lost personal devices	Define and communicate a clear policy on replacement, repair and compensation before implementation
Financial/ sustainability	Long-term affordability	BYOD allowances used in one campaign are not sustainable in future campaigns	Set realistic support levels; document cost assumptions; align with longer-term programme budgeting
Reputational	Community trust	Communities become concerned about data misuse when campaign workers use personal phones	Conduct community sensitization; use clear consent scripts and privacy messages; monitor and respond to rumours quickly



3. POLICY, PRIVACY AND SECURITY

This section sets out the governance framework for using personal devices in ITN campaigns. It covers BYOD policy development, ideally aligned with Ministry of Health policies where they exist and adapted as needed for programme- or campaign-specific require-

ments. This includes acceptable use rules, security standards, data governance and incident response. Clear governance protects campaign data, the workers and the communities the campaign serves.

3.1 Developing the BYOD policy

A BYOD policy sets the conditions under which personal devices may be used for campaign work. It should be drafted, endorsed by NMP leadership, legally reviewed where needed, and made available in the main languages used in the campaign area before enrolment begins. A sample Policy and Terms of Use is provided in [Annex 4](#).

At a minimum, the policy should define:

- Who may participate and which devices and campaign functions are covered.
- What users may and may not do on personal devices used for campaign work.

- Minimum device and security requirements.
- Data handling requirements, including storage, transmission, retention and deletion.
- Support, compensation and liability arrangements.
- Incident reporting and response procedures.
- Consequences for non-compliance.

The policy should be explained verbally during training, not only shared in written form for signature. Workers should understand the rules and implications of BYOD before enrolment is completed.

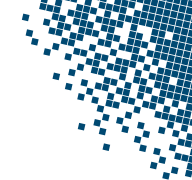
3.2 Define acceptable use and responsibilities

Users may deploy personal devices for approved campaign work only. This includes using programme-approved applications for assigned tasks, communicating with supervisors through approved channels, and accessing approved training or reference materials. Photography for campaign purposes is not recommended and should be permitted only where explicitly approved and where consent procedures are in place.

Users must not copy, export or share campaign data outside approved channels including through personal email, personal cloud storage or personal messaging applications. They must not take screenshots of data of any

community member, share login credentials or allow unauthorized persons to access campaign applications.

Workers should be provided with a standard oral consent script at training and should be able to explain to householders in their own words which information is being collected, why it is needed, and who will have access to it. By participating in BYOD, users accept the following responsibilities: keeping their device secure and updated; handling campaign data according to programme rules; reporting incidents immediately; cooperating with programme oversight; treating community members' data with respect. BYOD participation



should remain voluntary. Workers who opt out should not be penalized and should have access to an alternative arrangement.

The programme's management also has responsibilities. It should communicate BYOD rules clearly, provide orientation and support, apply the policy consistently and protect workers' privacy as far as possible while maintaining campaign data security.

3.3 Set minimum security and access controls

All devices used for BYOD should meet minimum security requirements. At a minimum, devices should have screen lock enabled, should not be rooted or jailbroken, should meet the approved operating system threshold, and should have the campaign application installed only from an approved source. Encryption should be enabled where supported. See the Device specification and verification checklist in [Annex 2](#).

Minimum access controls should also apply. These should include user authentication for the campaign application, role-based access so

users see only the data and functions they need, automatic session timeout after inactivity, and immediate deactivation of access when a user leaves the campaign or a device is compromised.

Campaign accounts must not be shared between users. Where a device is shared within a household, BYOD should only be used if the campaign application and account remain accessible solely to the enrolled user. If this cannot be assured, an alternative arrangement should be made.

3.4 Establish data governance and storage rules

NMPs should collect only the data needed for campaign operations. For each proposed form field, ask what specific programme decision or action requires these data. Remove any field for which there is no clear operational answer or where data will be used for reporting purposes only.

NMPs should define which data are collected; how long data remain on the device before synchronization; when local data should be cleared; and who may export or access datasets after the campaign.

Campaign data include all personal, sensitive and operational data collected during programme activities. The data should be stored within the application's encrypted container and synchronized automatically to the server when connectivity is available. Data should not

be retained on the device beyond what is operationally necessary — the preferred maximum is 72 hours after the last successful synchronization. Workers should not back up campaign data to personal cloud accounts, and app settings should prevent this where possible. The less data stored on the device at any given time, the lower the risk if a device is lost, shared or compromised.

Where supported, a remote deactivation or remote wipe approach for campaign data should be defined. This should apply in cases of device loss or theft, confirmed policy breach, serious security incident or campaign close-out. Where full MDM is not in use, the policy must make clear that remote wipe applies only to campaign data and not to the worker's personal content.

3.5 Incident response for lost, shared or compromised devices

NMPs should establish a simple incident reporting and response process before deployment begins. This should cover:

- Lost or stolen devices
- Failed login attempts or suspected account misuse
- Accidental sharing of data
- Device replacement during the campaign
- App malfunction affecting data integrity
- Suspected data breach or unauthorized access

All users should report any security incident, including loss or theft of devices, suspected data breaches, or unauthorized access, to their immediate supervisor or designated ICT support channel within a defined timeframe, and should cooperate fully with incident response procedures.

At a minimum, campaign access should be disabled without delay where needed, replacement devices should be re-verified before use, and all incidents should be logged and reviewed.

Where device sharing is common, programmes should assess whether BYOD is appropriate for that cadre or whether additional safeguards or alternative arrangements are required.

*Survey on mobile phone penetration and usage.
© Togo CDM 2014*



4. IMPLEMENTATION OF BYOD

This section describes the practical steps for implementing BYOD in an ITN campaign. Before roll-out, NMPs should confirm that the platform is suitable, the policy is in place, device

readiness has been assessed, and the required budget has been approved. The steps described in [Section 1.2](#) should be completed before implementation begins.

4.1 Fallback arrangements

BYOD should never be the only operational option. Fallback (alternative) arrangements must be developed as part of the campaign digitalization planning during macroplanning, not as an afterthought.

Fallback should be activated when:

- A device fails verification or is lost, stolen or damaged
- The app does not function reliably or connectivity prevents operational use

- The user opts out of BYOD

Fallback options may include:

- Loaner or programme-owned devices
- Reassignment of the user to a non-BYOD role
- Temporary paper-based recording with later data entry
- Supervisor-assisted submission where appropriate

4.2 Training

Ensure all device owners attend training sessions with their registered devices. Training should be practical and role-specific. It should cover both use of the application and the operational rules for BYOD.

At a minimum, users should be trained on:

- How to log in and access the correct forms
- How to work offline and when to synchronize
- How to protect the device and campaign data
- What to do and who to contact if the app fails, the device is lost, or sync does not work
- Who to contact for technical support
- Campaign standard operating procedures (SOPs)

Supervisors should receive additional training on device verification, sync monitoring, issue escalation and fallback activation.

In addition to the campaign SOPs, field worker training must cover:

- BYOD policy overview: what workers are agreeing to, what will be provided through the programme and what their rights are, including the right to opt out
- Escalation procedure: who to call for what problem; helpdesk contact numbers, etc.
- Consent script practice: role-play exercise where workers practise explaining to householders why data are being collected, but explaining in their own words



4.3 Support and supervision during implementation

BYOD requires active support during implementation, especially where devices vary in age, quality and configuration. NMPs should establish a tiered support structure covering field, district and national levels, such as:

- Field-level support for setup, login and basic troubleshooting
- District-level support for account, sync and app issues
- National or partner-level support for platform outages, data issues and security incidents

Supervisors should routinely monitor:

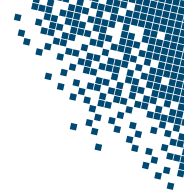
- Whether enrolled users are active
- Whether devices are synchronizing on time
- Whether data quality issues are increasing
- Whether any users need to switch to fallback arrangements

4.4 Daily operational controls

During implementation, the following operational controls should be applied, as appropriate to the worker cadre, responsibilities, and level of access to campaign systems and data.

- Users should sync according to the defined schedule
- Supervisors should review non-syncing users each day
- Duplicate checks and exception reports should be monitored
- Stock, distribution and supervision data should be reviewed for completeness
- Unresolved technical issues should be escalated quickly

Programmes should keep these controls simple and aligned with existing campaign management processes.



4.5 Post-campaign device closeout

At the end of the campaign, programmes should ensure that BYOD access is properly closed. Device closeout should be systematic and documented, as in Table 7.

Table 7: Post-campaign device closeout process

Step	Action	Verification
Remote logout	IT officer remotely logs out all enrolled accounts in the platform administration console.	Platform administration console shows all accounts as logged out.
App removal confirmation	Supervisor confirms app is removed from device during final field visit or via video call.	Supervisor completes device closeout.
Data deletion verification	Worker confirms no campaign data remain in any app, file or cloud backup on their device.	Signed confirmation on closeout checklist.
Random post-campaign check	IT officer selects 10% of workers for an additional random verification check within 14 days.	Spot-check log maintained.
Device inventory closure	Loaner devices should be returned after each campaign, recorded in inventory, securely stored, and maintained for reuse in future campaigns or other programme activities, with ongoing inventory management.	Final inventory signed by District IT officer.

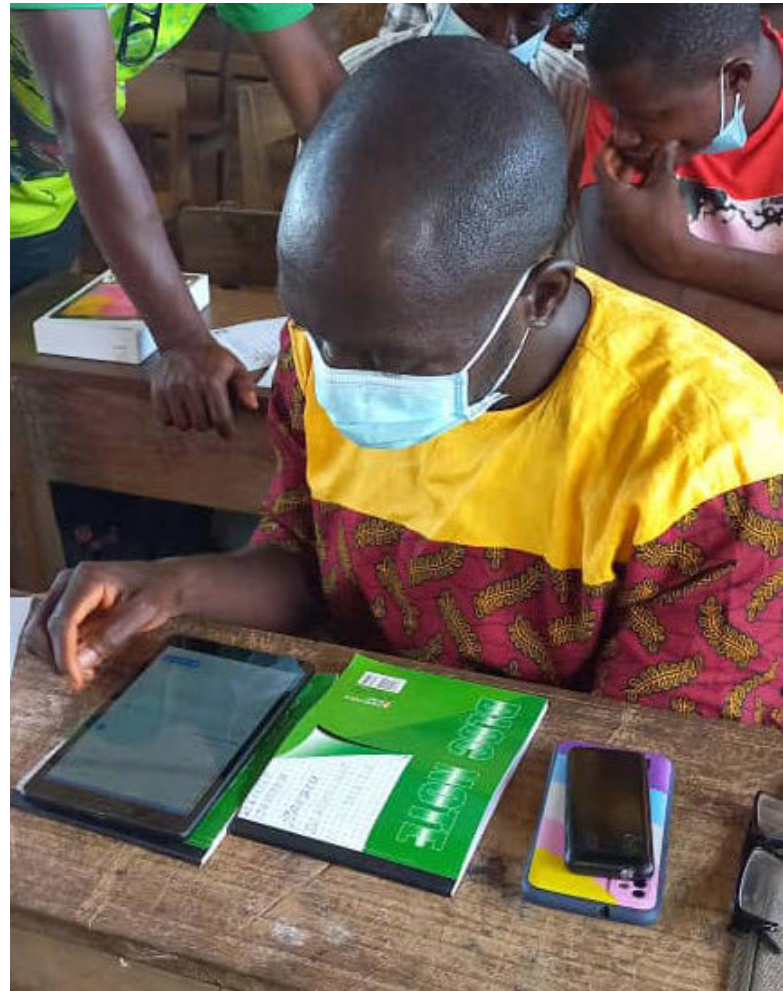
5. CONCLUSION

Programmes considering or scaling up BYOD for ITN campaign digitalization should take a deliberate and phased approach. BYOD should only be used where the minimum policy, technical, operational and equity conditions are in place. It should not be adopted as a default solution or scaled up based on convenience alone.

BYOD can offer important operational and cost advantages for ITN campaign digitalization, but only when it is introduced with a clear policy, realistic readiness assessment, appropriate safeguards and active monitoring. A structured, evidence-based approach will help NMPs use BYOD where it adds value while protecting data, supporting workers and maintaining implementation quality.

References

Doargajudhur, M. S., & Dell, P. (2020). The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation. *Journal of Computer Information Systems*, 60(6), 518–529. <https://doi.org/10.1080/08874417.2018.1543001>



Guinea campaign 2022

ANNEX 1: BYOD readiness assessment checklist

(Also available as an adaptable tool in MS Word)

Complete this checklist during campaign design before platform selection and budgeting.

#	Question	Response	Notes / comments
Legal, policy and data protection			
1	Does national law or the Data Protection Authority permit processing the relevant data categories on personal devices?	☐ Yes ☐ No ☐ In progress	
2	Has a Data Protection Impact Assessment been completed where higher-risk data are involved?	☐ Yes ☐ No ☐ In progress	
3	Has the BYOD policy been drafted, legally reviewed and endorsed by the NMP and implementing partners?	☐ Yes ☐ No ☐ In progress	
4	Has the policy been translated into the main campaign languages?	☐ Yes ☐ No ☐ In progress	
Device landscape and requirements			
5	Has a device census been conducted covering at least 80% of target campaign workers?	☐ Yes ☐ No ☐ In progress	
6	Do at least 85% of census devices meet the minimum specifications?	☐ Yes ☐ No ☐ In progress	
7	Has the application been tested on at least three representative low-end device models?	☐ Yes ☐ No ☐ In progress	

#	Question	Response	Notes / comments
Equity, inclusion and opt-out			
8	Has digital literacy been assessed for the target campaign workers?	☐ Yes ☐ No ☐ In progress	
9	Has readiness been assessed disaggregated by sex, age, cadre and geography?	☐ Yes ☐ No ☐ In progress	
10	Is a loaner pool of at least 5% of the BYOD workforce budgeted?	☐ Yes ☐ No ☐ In progress	
11	Are opt-out alternatives documented and communicated to all workers?	☐ Yes ☐ No ☐ In progress	
Connectivity, security and platform			
12	Does the application function fully offline for all essential workflows, with 2–3 days of local storage?	☐ Yes ☐ No ☐ In progress	
13	Are app-level controls confirmed — encryption, authentication, role-based access and session timeout?	☐ Yes ☐ No ☐ In progress	
14	Can remote logout / de-authentication be confirmed for all enrolled device types?	☐ Yes ☐ No ☐ In progress	
Cost and compensation			
15	Has a full BYOD versus programme-owned device cost comparison been completed?	☐ Yes ☐ No ☐ In progress	
16	Is a reimbursement or compensation model defined and communicated before roll-out?	☐ Yes ☐ No ☐ In progress	

#	Question	Response	Notes / comments
Risk and implementation readiness			
17	Have BYOD risks been assessed, with residual high or critical risks resolved or formally accepted?	☐ Yes ☐ No ☐ In progress	
18	Will BYOD be piloted with defined scale-up criteria before full roll-out?	☐ Yes ☐ No ☐ In progress	

Summary	
Comments	
Readiness rating	☐ Ready ☐ Ready with gaps ☐ Not ready
Critical gaps to close before proceeding	
Completed by	
Date	
Reviewed by (NMP or IP focal point)	

ANNEX 2: BYOD enrolment, device verification and consent form

(Also available as an adaptable tool in Excel)

Complete one form per enrolled user. Collect at training before app installation or, where possible, in advance of training. Store signed copies with the district coordinator and NMP digitalization lead.

Section 1 — Worker information			
Full name			
Sex	☐ Female ☐ Male ☐ Other		
Position / role in ITN campaign			
Organization (if applicable)			
District/facility/community	District	Facility	Community
Phone number (primary)			
Email (if applicable)			
Section 2 — Device identification and specification check (completed by IT officer/supervisor)			
Item	Recorded detail	Minimum requirement	Result
Device type		Smartphone or tablet	☐ Pass ☐ Fail
Make/brand and model		Record for inventory	—
Operating system and version		Android 8.0+ (API 26+) or iOS 13+	☐ Pass ☐ Fail
RAM		2 GB minimum	☐ Pass ☐ Fail

Free internal storage		2 GB before app installation	☐ Pass ☐ Fail
Battery (full working day)		6–8 hours minimum; assess actual health	☐ Pass ☐ Cond. ☐ Fail
Screen size		5.0 inches minimum	☐ Pass ☐ Fail
Mobile network		2G minimum; 3G preferred	☐ Pass ☐ Fail
GPS/location services		Functional where app captures location	☐ Pass ☐ N/A
Camera		Functional where app scans QR / barcode	☐ Pass ☐ N/A
IMEI/serial number		Optional	—

Record the actual detail in the middle column and mark the result. A device must pass all applicable items to be approved.

Section 3 — Security, exclusion and functional checks (completed by IT officer/supervisor)

Check	Requirement	Result
Screen lock active	PIN, password, pattern or biometric confirmed active	☐ Pass ☐ Fail
Device NOT rooted or jailbroken	No SuperSU, Magisk or jailbreak indicators. Absolute exclusion criterion.	☐ Pass ☐ FAIL
Operating system updated	Latest available version where feasible	☐ Yes ☐ No
Encryption active	Full-disk or app-level encryption confirmed	☐ Pass ☐ Fail
Campaign app installs and runs	App opens correct form and completes a test submission	☐ Pass ☐ Fail
Remote de-authentication confirmed	IT officer confirms remote logout works for this account	☐ Pass ☐ Fail

A rooted or jailbroken device is an absolute exclusion criterion and cannot be enrolled, regardless of other results

Section 4 — Worker declaration and consent (completed by the worker)

The device described above is my personal property or under my control.	☐ Confirmed
I have read, understood and agree to comply with the BYOD Policy and Terms of Use (Annex 4).	☐ Confirmed
I understand that campaign applications and data may be remotely disabled or removed by the programme.	☐ Confirmed
I will report loss, theft or suspected misuse of my device or campaign data immediately.	☐ Confirmed
I understand that BYOD participation is voluntary, and that opting out will not affect my campaign standing or compensation.	☐ Confirmed
By signing below I confirm the declarations above. This signature also records my acknowledgement of the BYOD Policy and Terms of Use.	
Worker signature	Date

Section 5 — Programme approval and enrolment decision (internal use only)

Device meets minimum technical and security requirements	☐ Yes ☐ No — Reason:
Enrolled by (name of IT officer or programme representative)	
Date enrolled	
BYOD user ID/ device ID assigned in system	
Approver signature	

ANNEX 3: Device inventory template

(also available as an adaptable tool in Excel)

Maintain as a shared spreadsheet accessible to district IT officers and the NMP digitalization lead.
Update in real time throughout the campaign.

BYOD user ID	Full name	Role	District	Device make/model	OS and version	Meets min. specs	Date enrolled	Date de-enrolled	Notes
BYOD-0001	Example Name	HHR personnel	[District]	Samsung A10	Android 11	Yes	DD-MM-YYYY		
BYOD-0002									
BYOD-0003									

ANNEX 4: Sample BYOD policy and terms of use for ITN campaigns

(Also available as an adaptable tool in MS Word)

Replace all text in [brackets] with country- or programme-specific information before use. Legal review is mandatory before finalizing

and distributing this policy. Translate into all languages used in the campaign area.

1. Purpose

This Bring Your Own Device (BYOD) Policy sets out the conditions under which personally owned mobile devices may be used to support the [Country] ITN campaign [Year] coordinated by the [Ministry of Health/national malaria pro-

gramme] ("the programme"). The purpose is to enable the safe and effective use of personal devices for approved campaign activities while protecting programme data, workers and ITN recipients.

2. Scope

This policy applies to:

- All staff, volunteers and contractors ("users") participating in the [Country] ITN campaign [Year] who use personal devices for campaign work
- All personal smartphones, tablets or laptops enrolled to access campaign applications or campaign data

This policy does not cover back-end servers, hosting infrastructure or programme-owned devices, which are governed under separate ICT and data protection policies.

3. Definitions

Term	Definition
BYOD	The use of personally owned devices for approved campaign work under this policy.
Personal device	A smartphone, tablet or laptop owned by the user, not by the programme.
Campaign application	An approved digital tool used for campaign activities, such as household registration, distribution recording, supervision or stock reporting.
Programme-owned device	A device purchased and managed by the programme or an implementing partner.

4. Eligibility

A user may participate in BYOD only if all the following conditions are met:

- The user is formally engaged in the campaign
- The device meets the minimum technical and security requirements set out in [Annex 2](#)
- The user has completed the required BYOD training or orientation as verified by the online post-test
- The user has signed this policy and the BYOD enrolment and consent form in [Annex 2](#)

BYOD participation is voluntary. Workers who decline to use a personal device must not be penalized and must have access to an alternative arrangement. The programme may refuse, suspend or revoke BYOD participation at any time for security, legal or operational reasons.

5. Acceptable use

Users may use personal devices for approved campaign tasks only. These include (for example):

- Household registration
- ITN distribution recording
- Supervision and quality assurance checklists
- Stock and logistics updates
- Approved training and reference materials

Users may also use approved communication channels for campaign coordination with supervisors and colleagues.

Users must not use personal devices enrolled under BYOD to:

- Share campaign data through unapproved applications or channels

- Copy, export or store campaign data outside approved applications
- Take screenshots of recipient lists, household data or any information containing personal identifiers
- Allow unauthorized persons to access campaign applications or data
- Harass, abuse or discriminate against recipients, colleagues or community members
- Access illegal, harmful or inappropriate content using programme-funded data

Use of social media, streaming and other non-work services during campaign activities should be restricted where programme-funded data are provided.

6. Security requirements

Users must ensure that:

- The device is protected by a PIN, password, pattern or biometric lock
- The device locks automatically after no more than five minutes of inactivity
- The operating system and campaign applications are kept up to date
- The device is not rooted or jailbroken
- Only approved campaign applications are used for campaign work
- Campaign data are not copied, exported or shared outside approved channels

Where feasible, the programme may apply technical controls such as app-level security settings, work profiles or mobile device management tools.

7. Data protection and privacy

Users must collect and process only the data required for campaign activities, in accordance with programme procedures and applicable [Country] data protection law.

Users must not store campaign data in personal cloud storage, personal email, personal messaging applications or other unapproved locations.

The programme will:

- Apply data minimization principles and collect only data necessary for campaign operations
- Use the least intrusive technical controls necessary to protect campaign data
- Avoid access to personal content on the device, except where permitted by law and strictly necessary to investigate a serious security incident

Workers will be provided with an approved oral consent script for communicating with households about which data are being collected, why they are needed, and who will have access to them.

8. Support, reimbursement and equipment

The programme will:

- Provide training and basic technical support for approved campaign applications
- Provide data or airtime support, or a defined allowance, for reasonable campaign-related use, in line with campaign procedures
- Maintain a limited pool of programme-owned loaner devices for users without suitable personal devices or for fallback purposes

(Depending on policy decisions) full replacement of a lost, stolen or damaged personal device is not guaranteed. Any support provided will depend on programme rules, available resources and the documented circumstances of the incident.

9. User responsibilities

By participating in BYOD, users agree to:

- Comply with this policy and related programme procedures
- Keep their device secure, updated and in good working condition
- Report lost or stolen devices, suspected data breaches and policy violations immediately
- Allow the programme to remove campaign applications and data at the end of the campaign or engagement
- Allow the programme to disable access or remotely remove campaign data in the event of loss, theft or a serious security incident

Users must not allow unauthorized individuals to use their device to access campaign applications or data.

10. Programme responsibilities

The programme will:

- Communicate BYOD rules, risks and responsibilities clearly and in a language workers understand
- Provide training materials and support contacts before the campaign begins
- Apply this policy consistently and fairly across all users and cadres
- Take reasonable steps to protect both campaign data and the privacy of workers' personal device content

11. Non-compliance

Failure to comply with this policy may result in:

- Suspension or removal of BYOD access
- Deactivation of campaign application accounts
- Disciplinary action in line with applicable staff or volunteer procedures
- Referral to relevant authorities where required by law

12. User acknowledgement

This form should be signed before device enrolment is completed and before access to campaign applications is granted.

Field	Response
I, [Name], confirm that I have read and understood the BYOD policy and terms of use for the [Country] ITN campaign [Year]. I agree to comply with these requirements and understand the responsibilities associated with using my personal device for campaign work.	
Full name	
Position/role	
Organization (if applicable)	
Phone number	
Device make and model	
IMEI/serial number (optional)	
Signature	
Date	



AMP CONTACTS

To join the weekly AMP conference call each Wednesday at 10:00 AM Eastern time (16.00 PM CET) use the following Zoom meeting line:

<https://us06web.zoom.us/j/88935481892?pwd=h3cuJ3x5LOsR58YXcEaub8ULqu5LMj.1>

You can find your local number to join the weekly call:

<https://zoom.us/j/88935481892>

To be added to the AMP mailing list visit:

<https://allianceformalariaprevention.com/join-us>

To contact AMP or join an AMP working group please e-mail:

info@allianceformalariaprevention.com

For further information please go to the AMP website:

<https://allianceformalariaprevention.com>