

COOKIES AND SIMILAR TECHNOLOGIES POLICY

Deploying, classifying, consenting and disclosing tracking
technologies

CLASSIFICATION: INTERNAL — STAFF USE ONLY

Document Reference	PRIV-CST-01
Parent Policy	Internal Privacy and Data Protection Policy (PRIV-POL-01)
Owner	Data Protection Officer, jointly with Head of Marketing / Head of IT
Approval	DPO (updatable without Board re-approval, provided it does not alter an obligation stated in the Core Policy)
Version / Effective	1.0 / 01/12/2025
Review Cycle	Annually, and on every quarterly cookie scan that identifies an unregistered technology
Applies To	Marketing, Web, Product, Engineering and Analytics teams; anyone requesting a tag, pixel or SDK

1. Purpose and Scope

This policy outlines how we categorise, deploy, and govern cookies and tracking technologies across our website and web applications to protect user privacy.

Cookies are small text files or similar technologies placed on a user's device when they visit a website. They may enable a website to remember user preferences, maintain security and functionality, analyse website use, or support other services. Cookies may collect information such as: IP address; device and browser information; pages visited and interactions with the website; language and preferences; approximate location; and online identifiers.

Where such information relates to or can reasonably be linked to an identifiable individual, it will be treated as personal data and processed in accordance with the Nigeria Data Protection Act (NDPA).

2. Default Position

The Organisation's default position is that it does not deploy cookies or similar technologies. Where a business case arises to deploy a functional, analytics, targeting or social technology, the requirements of this Policy apply in full.

3. Legal Position

Information stored on or read from a user's device, and the personal data derived from it, is processed under the NDPA framework and requires an identified lawful basis. Consent is the basis relied upon for all non-essential cookie technologies. Where technology is strictly necessary to deliver a service, the user has requested, the Organisation may rely on an alternative basis — but the technology must still be disclosed in the Cookie Notice.

4. Categories and Consent Requirements

All tracking technologies must be classified into one of the following categories and adhere strictly to these consent rules:

Category	Definition and examples	Consent
Strictly necessary	Required to deliver a service the user has expressly requested, or for security. Examples: session and authentication cookies, load balancing, CSRF tokens, fraud prevention, shopping basket state, and the cookie that stores the user's own consent choices.	Not required. Disclosure in the Cookie Notice is still required. Must not be pre-selected as a proxy for other purposes.
Functional/preference	Remember user choices to improve experience but are not required for the service to work. Examples: language selection, region, interface preferences, chat widgets.	Required. Off by default.
Performance/analytics	Measure how users interact with the service. Examples: page analytics, error monitoring with user-level data, A/B testing, session replay, heat-mapping.	Required. Off by default.
Targeting/advertising	Build profiles, retarget users, measure campaign performance, or share data with advertising partners. Examples: advertising pixels, conversion APIs, audience-matching tags, affiliate tracking.	Required. Off by default.
Social media/embedded content	Third-party embeds that set their own cookies. Examples: video players, social share widgets, embedded maps and forms.	Required. Off by default.

Consent to non-essential technologies must be freely given, specific, informed and unambiguous, and given by a clear affirmative act. A readily accessible mechanism, such as cookie settings, shall be provided through which users can change their preferences.

5. Operational Requirements for Teams

A. Consent Architecture (Web/App Developers):

- **Default State:** All non-essential scripts, tags, and pixels MUST be paused/blocked by default until the user clicks "Accept".
- **No Dark Patterns:** No pre-checked boxes. "Scrolling" or "continuing to use the site" does not constitute legal consent.
- **Easy Opt-Out:** Users must be able to access a "Cookie Preferences" link in the footer to withdraw or change their consent just as easily as they gave it.

B. Data Logging & Retention (IT & Data Engineering):

- **Consent Logs:** The Consent Management Platform (CMP) must log the timestamp, user ID (or anonymous identifier), and consent state for audit purposes.
- **Lifespan:** Persistent cookies must have a defined expiration date. They should not last longer than necessary for their purpose (maximum 12 months before re-consenting).

C. Third-Party Vendors (Marketing & Procurement):

- Before adding any new third-party tracker (e.g., ad network, analytics tool), the vendor must be vetted by the DPO for NDPA compliance, especially regarding cross-border data transfers.

6. Governance and Audit

- Quarterly Audits: The IT team will conduct automated cookie scans every quarter to identify unclassified, rogue, or expired third-party cookies.
- Policy Updates: Any changes to the web trackers must be reflected in the public-facing Privacy/Cookie Notice immediately.

7. External-Facing Cookie Notice

When we deploy cookies or similar technologies, a public-facing cookie notice shall be published explaining:

- What cookies are
- The categories of cookies used
- Their purposes
- The organisation responsible for their use
- Relevant third parties
- The applicable lawful bases

- How users can accept, reject or manage cookies
- How users can withdraw consent
- Who to contact.

8. Cookie Banners

Where cookies are used, a clear and conspicuous cookie banner should be displayed to first-time visitors of our website. The banner should:

- inform the user that cookies or similar tracking technologies are being used;
- explain their main purposes in clear and simple language;
- identify us as the organisation responsible for their use;
- provide the user with a clear choice to accept or reject non-essential cookies;
- provide an option to manage cookie preferences where appropriate; and
- explain how the user can withdraw or change consent.

The cookie banner must not use deceptive design, pre-ticked consent boxes or other mechanisms intended to make users inadvertently accept non-essential cookies.

9. Contact and Escalation

For questions on categorising a new tracker, implementing the CMP, or reporting a compliance breach, contact the DPO at dpo@heckerbella.com.

Name: Abdulganeey Oyegbemi

Designation: Data Protection Officer

Sign: 

Date: 8th Dec. 2025