Staples

## Staples Digital Solutions

# Biometrics Information Policy

| | |
|---|---|
| **Document ID #** | POL10307 |
| **Version #** | 2.3 |
| **Data Classification** | Corporate |
| **Last Revised Date** | 2/18/26 |
| **Next Revised Date** | 10/1/26 |
| **Contact E-mail** | Privacy@staples.com |
| **Document Owner** | Justin Tuttleman |

## Document History

| Version | Date | Author of Changes | Description |
|---|---|---|---|
| 2.3 | 2/18/26 | Galina McDonnell<br>Justin Tuttleman | Updates for new Biometrics Laws |
| 2.2 | 1/14/26 | Galina McDonnell | Updated for Applicant and Workforce due to 1Kosmos implementation |
| 2.1 | 12/4/24 | Samir Khalifa | Updated with new template |
| 2.0 | 10/1/24 | Danielle Johnson | Complete version and rewrite of the original |
| | | | |

# Table of Contents

# 1. Background/Purpose

Staples Workforce may be subject to collection and processing of Biometric Information (as defined below) for security, safety, and compliance purposes, including Staples network credential resets and/or facial recognition in certain facilities in support of building access controls.

The purpose of this Biometrics Information Policy is to set forth applicable principles and practices for the collection, use, storage, and destruction of such Biometric Information by Staples (as defined below) and its third-party service providers.

It is Staples' policy to protect, use, store, and dispose of Biometric Information in accordance with all applicable laws and regulations.

# 2. Scope

This policy applies to Staples, Inc., its subsidiaries, and its affiliated companies (referred to collectively as "Staples").

This policy applies to all Staples associates, contractors, temporary workers, applicants and other individuals working on our behalf, regardless of geographic location and/or level of responsibility, who may collect, use, store, or have access to Staples' Biometric Information, and/or whose Biometric Information may be collected (referred to collectively as "Workforce").

This policy applies to all third parties that Staples may engage to collect, store, or process Biometric Information on its behalf.

This policy covers all types of Biometric Information that we collect, store, or process.

# 3. Policy

## 1. Collection of Biometric Information

### 1.1 Lawful Purpose

- Biometric Information may be collected only for lawful purposes that are directly related to the security, safety, and compliance functions and activities of Staples, such as facility access controls and network credential resets.
- The collection of Biometric Information must be limited to that which is reasonably necessary for the intended purpose.
- Where required by law (or otherwise appropriate in its discretion), Staples will conduct a privacy impact assessment before the implementation of new Biometric Information collection practices or systems/technology, or before making significant changes to the existing implementations.

### 1.2 Notice and Consent

- Where required by law (or otherwise appropriate in its discretion), Staples will provide written notice ("Notice") to Workforce members and obtain their written consent prior to collecting or otherwise obtaining their Biometric Information.
- The Notice will describe the type of Biometric Information being collected, stored, and used, the purpose and length of term for such collection, storage, and use, and any other information that may be legally required in such a notice.

- The Notice will include a consent form ("Consent Form") for the Workforce member to provide their written consent to the collection and use of their Biometric Information. Completion of this Consent Form may be required as a condition of continued employment or work with Staples.
- Workforce members may revoke their consent to the collection or use of their Biometric Information by notifying Staples in writing. Please note, however, that where the collection or use of Biometric Information is required as a condition of continued employment or work with Staples, such revocation of consent may result in the termination of employment or work with Staples where permitted by law.

## 2. Use and Disclosure of Biometric Information

### 2.1 Restrictions

- Biometric Information may be used and disclosed only for lawful purposes that are directly related to the security, safety, and compliance functions and activities of Staples, such as facility access controls and network credential resets.
- Staples will not sell, lease, trade, or otherwise profit from the Biometric Information of its Workforce.
- Access to Biometric Information will be limited to authorized Workforce members and authorized third-party personnel only. All such Workforce members and third-party personnel must comply with this policy in their use of Biometric Information.
- Staples will not disclose or disseminate Biometric Information to anyone other than its Workforce members and third-party service providers unless disclosure is required by law or pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

## 3. Protection of Biometric Information

### 3.1 At Rest and In Transmission

- Biometric Information will be stored and transmitted in a manner that provides a reasonable standard of care designed for sensitive personal information and designed to protect against unauthorized access, manipulation, use, or disclosure.
- Staples will implement administrative, physical, and technical safeguards reasonably designed to protect the security, confidentiality, integrity, and availability of Biometric Information.
- These safeguards will be equivalent to or more protective than the manner in which Staples is required to store, transmit, and protect other data classified as Highly Restricted (per the Staples Privacy and Information Management Policy).

## 4. Retention and Destruction of Biometric Information

### 4.1 Retention

- Staples will retain Biometric Information only until the earliest of the following dates:
    - The date on which the purpose for collecting such Biometric Information has been fully satisfied and therefore retention of the Biometric Information is no longer necessary, adequate, or relevant to the purpose; or
    - 12 months after the Workforce member last interacted with Staples.
- In determining whether the purpose for collecting Biometric Information has been fully satisfied, Staples will consider (a) whether the Biometric Information may continue to be needed for the security, safety, and compliance functions and activities for which it is used, such as facility access controls and network credential resets; (b) whether the Biometric Information may be needed for a reasonable period of time thereafter, not to exceed 12 months, for audits and investigations of such security, safety, and compliance functions; and (c) whether any further reasonable period of time, not to exceed 45 days

after the completion of (a) and (b) above, may be needed to accomplish the permanent destruction of the Biometric Information as described below, which 45-day period may be extended for 45 additional days if reasonably necessary taking into account the complexity and amount of Biometric Information required to be deleted.

- Notwithstanding the foregoing, Staples may retain Biometric Information for a longer period of time if required by law to do so.

**4.2 Destruction**

- Staples will permanently destroy Biometric Information after the purpose for its collection has been satisfied.
- Biometric Information in electronic/digital format will be deleted using secure destruction techniques designed to prevent the recovery of deleted data/files.
- Biometric Information in hard-copy format will be securely shredded.

### 5. Incident Response

**5.1 Breach of Biometric Information**

- In the event of a breach of Biometric Information, Staples will respond in accordance with the Incident Response Plan.

## 4. Definitions

- **Biometric Information**: Data generated by or derived from the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that are used to uniquely identify an individual, including but not limited to fingerprints, facial mapping/geometry/templates, voiceprints, iris or retina scans, digital/physical photograph, audio/voice recording, etc.
- **Collect:** To access, assemble, buy, rent, gather, procure, receive, capture, or otherwise obtain Biometric Information from any source.

## 5. Enforcement

This policy will be reviewed periodically and may be updated to reflect changes in the Biometric Information systems or technologies that we use, or in the applicable laws and regulations regarding Biometric Information. Any changes to this policy will be communicated to the relevant stakeholders and published on the Staples intranet.

Workforce members or third parties must notify their management or the Privacy Team (Privacy@Staples.com) immediately if they believe the company's systems or information may be at risk or if additional guidance is needed.

Workforce members or third parties working in a jurisdiction, business unit, or group that imposes additional privacy or security requirements (i.e., laws, policies, or procedures) also must comply with those requirements. In the event of any conflict between Staples policy requirements and relevant laws or regulations, the respective laws and/or regulations will govern.

Violations of this policy may result in disciplinary actions, up to and including termination of employment/contracts or other measures in accordance with the applicable working regulations, internal procedures, and laws of the applicable jurisdiction(s).

Waivers, deviations, and exceptions to this policy must be reviewed and approved by the Privacy Team. Policy exception or change requests can be submitted to Privacy@Staples.com.

## 6. References and Related Documents

- Staples Privacy and Information Management Policy