This policy is applicable to U.S. employees only, excluding employees in Puerto Rico.  If you are in Puerto Rico, click [here](https://agreementservice.svs.nike.com/rest/agreement?agreementType=privacyPolicy&uxId=com.nike.employee.pp&country=pr&language=es&requestType=redirect) for the policy for Puerto Rico employees.

For employees outside of the U.S. and Puerto Rico, click [here](https://agreementservice.svs.nike.com/rest/agreement?agreementType=privacyPolicy&uxId=com.nike.employee.pp&country=gb&language=en&requestType=redirect) for the global policy.

# ****Nike U.S. Employee Privacy Policy****

Last updated: April 2023

This Employee Privacy Policy (the “Policy”) is applicable to U.S. employees only (“employees” or “you”), excluding employees in Puerto Rico. Click  [here](https://agreementservice.svs.nike.com/rest/agreement?agreementType=privacyPolicy&uxId=com.nike.employee.pp&country=pr&language=es&requestType=redirect) for the policy for Puerto Rico employees.

As further described below, Nike collects and processes Personal Information that you provide to us as part of our employee on-boarding process. We also collect and process additional types of Personal Information about you throughout your employment with Nike to administer our human resources program; to comply with employment terms and conditions and applicable law in the fields of employment, social security, and workplace health and safety; to manage your participation in voluntary employee programs. You may contact Nike’s Privacy Office or Data Protection Officer by emailing [privacy.office@nike.com](mailto:privacy.office@nike.com).

If you are a resident of California, please see the Additional Information for [California Residents section](https://agreementservice.svs.nike.com/rest/CAResidents).

## 1. Introduction and Scope

1. Nike, Inc., Converse, Inc., and their affiliates, including your employer (collectively “Nike”, “we”, “us” or “our”) respect your privacy. We are committed to processing the Personal Information of our employees in compliance with applicable law and Nike policies. For the purpose of this Policy, “Personal Information” means (i) information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked (directly or indirectly) with a particular identified or identifiable individual, device, or household; and (ii) information defined as “Personal Data,” “Personal Information,” “Personally Identifiable Information” or a similar term under applicable law. Examples of Personal Information include but are not limited to an individual’s name, contact information, identification number(s), location information, online identifier(s) (e.g., IP address or device ID), online activity information (e.g., browsing history), biometric information, and payment information.
2. This Policy is intended to provide an overall description about how we collect and process employee Personal Information, however, our collection and processing of Personal Information may vary depending upon the circumstances, such as your role and responsibilities with us. This Policy also describes the measures we take to safeguard Personal Information and how employees can contact us with questions about our privacy practices. The entity responsible for the collection and processing of your Personal Information is your employer of record. If you have questions regarding the details of your employer, please review the terms and conditions of your employment or reach out to HR Direct.
3. This Policy applies to current and former full-time and part-time employees and interns of Nike (collectively “employees”).  This Policy does not apply to External Temporary Workers (“ETW”), independent contractors providing services to Nike, job applicants, or consumers.  It also does not apply to employees in the context of their personal use of our products and services, which are subject to different notices.  If you are an External Temporary Worker (“ETW”) or an independent contractor providing services to Nike, please contact your direct employer to inquire about its privacy and data protection practices.
4. Nike may provide additional privacy or data protection notices and policies to employees in specific functions, or who utilize specific tools or platforms, as appropriate. Nike may also provide additional privacy or data protection policies in jurisdictions where required for compliance with local law. The additional notice or policy will control to the extent there is a conflict with this Policy, with respect to your Personal Information that is subject to that notice or policy.  When you interact with our website, our privacy and data protection practices are as described in our website's privacy policy.
5. This Policy applies in addition to all other Nike corporate policies, including, but not limited to, Nike’s [Code of Conduct (“Inside the Lines”)](https://zero.nike.com/home/sites/insidethelines/), [Acceptable Use Policy](https://niketech.service-now.com/nikehr?id=nikehr_kb_article_view&sysparm_article=KB0032161): Electronic Communications and Devices, [Social Media Policy](https://niketech.service-now.com/nikehr?id=nikehr_kb_article_view&sysparm_article=KB0031541), Personal Data Handling Policy, Applicant Privacy Policy, and Enterprise Data Access Policy,  all of which are available on Zero.

## 2. Types of Personal Information We Collect and How We Use Them

We collect and process Personal Information about you for the purposes described below, including as far as necessary to manage the terms and conditions of your employment, to comply with legal obligations to which we are subject. This includes Nike’s legal defense and compliance with tax, finance, labor, social security and other applicable laws, or laws and orders requiring the disclosure of data to competent authorities in accordance with applicable law or court order. We also process your Personal Information to pursue the legitimate business interests of Nike . We use manual or automated methods to process your Personal Information.

###### Onboarding

We collect and process your Personal Information through the onboarding process to set up and administer your employment relationship, to comply with the legal obligations to which we are subject. This includes:

* + the information that you provided to us during the recruitment process, including your resume or curriculum vitae, application form, work history, education, degrees, academic records, languages and qualifications, references and any professional licenses, memberships, or certifications;
  + your basic contact and demographic information, including your name, address, telephone numbers (home, mobile/cell, work), email address, citizenship/nationality, date and place of birth, gender, and work permit information if applicable;
  + your government issued identifiers subject to the conditions of applicable law, such as your national ID details, tax identification number, social security or national insurance number, passport number, and, where required for your job, your driver’s license number;
  + your bank and financial details for salary/payroll purposes, such as your salary, other remuneration, your IBAN number or bank account number, and bank name, routing number and details;
  + information about your job and position, including the employee identification number, badge number, job title and description, department and manager, reporting lines, work location, cost center, business unit or group, work status such as full time or part time, working hours, probation period if applicable, and employment terms and conditions;
  + information for use of Nike network and devices if applicable, such as username, password, contact details, work telephone number and device data (computer, telephone, tablet ID number), company photo, if provided; and
  + information about your personal or family life, including marital status, dependents, beneficiaries and partner/spouse, and emergency contact information.

We may maintain the information we collect when we conduct pre-employment verification of your identity, address, or references and, where permitted by local law, the verification of background checks (including criminal or judicial data) about you, in accordance with [Nike’s Background Checks Policy](https://niketech.service-now.com/nikehr?id=nikehr_kb_article_view&sysparm_article=KB0031601).

###### 

###### Human Resources Management

We collect Personal Information that is generated during your employment as necessary to help manage your working relationship with Nike. This includes:

* + information about your working hours and leaves, including attendance, holiday/vacation, leaves or absences, travel and mobility;
  + economic and financial information for compensation and benefits, including your banking and account details for remuneration and compensation, information on raises and bonuses, your benefits package and information and details associated with pensions or insurance programs that may be offered in your country;
  + information related to your work evaluations and performance, including regular evaluation details, reviews and feedback, details about performance plans, and information associated with professional development such as trainings (both internal and external), courses, seminars and conferences, and succession planning information;
  + information collected for travel and expense purposes, such as credit card information, bank details (e.g., account and routing numbers, IBAN, etc.), booking and itinerary details, passport information (e.g., number, expiration, issuing authority, etc.), visa and immigration information, and travel preferences (e.g., seat preference, dietary restrictions, and frequent flyer and corporate memberships, if provided);
  + information associated with mobility, transfers and relocation (either upon hiring or as part of a transfer or work assignment), including family details, immigration status and nationality/citizenship, and tax and social security information.; and
  + information about your participation in and the administration of the Nike  Employee Stock Purchase Plan (ESPP –which is a voluntary incentive program, please also see paragraph 6) and bonus grants, including your contact information, national tax information (including national identifier), nationality, job title, shares and position, details of purchases and entitlements to shares awarded, cancelled, exercised, (un)vested or outstanding for implementing, administering and managing the ESPP.

###### 

###### Safety and Security

* We monitor our facilities and use CCTV for employee safety, security and other legitimate business purposes, such as loss prevention. The facilities that use CCTV display visible signage where this is required by applicable law. We may use camera footage or recordings in those facilities to protect the legitimate interests or to defend the legal rights of Nike as permitted by applicable law.
* We also process Personal Information associated with the protection of employee health and safety in workplaces, including contact details and other Personal Information (such as driver’s license details), as well as a description of the accident or injury and any remediation.
* Additionally, we process information about your use of Nike devices, technology and network to pursue our legitimate interest in securing our information and information systems. More information about these practices is described in Nike’s [Acceptable Use Policy](https://niketech.service-now.com/nikehr?id=nikehr_kb_article_view&sysparm_article=KB0032161).
* In exceptional cases, we may need to process your Personal Information if it is necessary to protect your vital interests such as in case an accident happens at work or during work business travel.

###### 

###### Offboarding

We collect and process Personal Information during offboarding to finalize the employment relationship and to comply with our legal obligations. This includes information associated with retirement and termination, such as details of retirement, resignation, layoffs/reorganization, including notice period, termination date, reason for leaving and termination, retirement, and pension administration arrangements.

###### 

###### Voluntary Programs

From time to time, we may offer voluntary employee programs that process Personal Information in which you may freely agree to participate.

###### 

###### Sensitive Personal Information Processing

During onboarding and throughout your employment relationship, we may collect sensitive Personal Information subject to the conditions of applicable law.  Our collection, use, and disclosure of sensitive Personal Information is generally limited to what is reasonable and proportionate to the purpose for which we collect it.  For example, you may need to provide us or our company doctor with medical information to allow us to manage illness, incapacity, or disability issues, or to make a reasonable accommodation. In some countries, you may provide us voluntarily with sensitive Personal Information, such as your race, ethnicity, religion or sexual orientation, for diversity and equal opportunities purposes and where required or permitted by law. We also may be required to collect sensitive data to comply with our legal requirements in the fields of employment, social security, social protection (e.g., wage liens, tax or social security number), and other applicable laws.

###### 

###### Compliance with Legal Obligations

We may use your Personal Information to comply with applicable legal obligations (such as determining hiring eligibility or responding to subpoenas and court orders) as well as assessments, reviews and reporting relating to such legal obligations, including under employment and labor laws and regulations, Social Security and tax laws, environmental regulations, workplace safety laws and regulations, and other applicable laws, regulations, opinions and guidance.

###### Defending and Protecting Rights

We may use your Personal Information to protect and defend our rights and interests and those of third parties, including to manage and respond to employee and other legal disputes, to respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, including without limitation, Nike’s trade secrets and other intellectual property; the rights, interests, property, health, safety and reputation of Nike and its workforce; and the rights, interests, property, health or safety of others, including in the context of anticipated or actual litigation with third parties.

###### Mergers, Acquisitions and Other Business Transactions

We may use your Personal Information for purposes of planning, due diligence and implementation of commercial transactions, such as mergers, acquisitions, asset sales or transfers, financings, bankruptcy or reorganization or other similar business transactions.

###### Auditing, Accounting, Reporting and Corporate Governance

We may use your Personal Information for purposes relating to financial, tax and accounting audits; audits and assessments of our business operations, including without limitation assessing the effectiveness of Nike's business processes and measuring employee engagement; ensuring business continuity in case of absence or departures from Nike; problem resolution (e.g., internal reviews, grievances); management of whistleblowing channels; internal investigations; compliance (including conflicts of interest); risk management and security purposes, including security controls and financial controls; compliance with applicable laws, regulations and legal obligations; and for other internal business purposes such as administering our records retention program.

###### Other Legitimate Business Purposes

We may use your Personal Information based on our legitimate interest as necessary to conduct investigations, defend Nike’s legal interests, exercise claims or litigation, and comply with judicial or regulatory orders. We may also need to maintain disciplinary and grievance records (such as records of allegations, investigations or audits), as permitted or required by law. We process Personal Information as necessary to operate Nike’s Speak Up Portal in accordance with Nike’s [Code of Conduct (Inside the Lines)](https://zero.nike.com/home/sites/insidethelines/).

## 3. Sources of Personal information

1. We strive to obtain Personal Information directly from you to keep it accurate, up to date and relevant. Collection of Personal Information may occur during the job application process, during the employee on-boarding process, or on an ad hoc basis throughout your employment.
2. We also receive Personal Information about you from your line manager (for example, for performance or annual reviews) or from other colleagues (for example, in the context of periodic reviews or evaluations or if conducting a disciplinary investigation). From time to time, we may receive Personal Information about you from other third parties, for example customers, store partners, companies such as benefits providers, educational institutions, former employers, professional networking websites, professional references, members of the public and regulatory bodies.  We may also receive Personal Information from our websites, apps, systems, and network, as well as our third-party service providers.

## 4. Disclosures of Personal information

1. We share your Personal Information with other Nike entities for administrative purposes where required to run global processes, carry out group-wide reporting, or make decisions about senior hires or promotions based on our legitimate interest to administer our HR operations. This is typically administered by our HR Direct service centers serving Asia, Europe, and the rest of the world; these are located in Singapore (Nike Trading Company B.V., Singapore Branch), the Netherlands (Nike European Operations Netherlands B.V.) and the U.S.A. (Nike, Inc.) respectively.
2. As a global company, Nike relies on service providers and vendors that provide products and services.  Nike may disclose the categories of Personal Information listed above to these third parties based on our legitimate interest to engage third parties where necessary for the purpose of achieving the objectives outlined above. These include accountants, law firms and legal service providers, tax or financial professionals, payroll and benefits providers, relocation companies, pension and insurance companies, human resources specialists, consultants, contractors, IT support and storage providers.  We do not sell or share your Personal Information for advertising purposes.
   1. Our third-party service providers may have access to your Personal Information to perform certain functions or may host your Personal Information as part of a “cloud based” solution used by Nike employees. Nike uses third-party service providers that provide sufficient guarantees for the protection of your Personal Information. All vendors are to undergo Nike’s vendor risk assessment. Nike  requires third-party service providers by contract to implement appropriate data security and confidentiality obligations, in accordance with applicable law.
3. Some third parties to whom we may disclose Personal Information, for instance health insurance providers and pension scheme trustees, are data controllers in their own right, and you should refer to their own privacy policies in respect of how they use your Personal Information.
4. We may disclose Personal Information to third parties to comply with our legal and compliance obligations and to respond to legal process. For example, we may disclose information in response to subpoenas, court orders, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements.  This may include regulators, government entities, and law enforcement as required by law or legal process.
5. If we or our affiliates are or may be acquired by, merged with, or invested in by another company, or if any of our assets are or may be transferred to another company, whether as part of a sale, bankruptcy or insolvency proceeding or otherwise, we may transfer the Personal Information we have collected from you to the other company.  We may also share certain Personal Information as necessary prior to the completion of such a transaction or corporate transactions, such as financings or restructurings, to lenders, auditors, and third-party advisors, including attorneys and consultants, as part of due diligence or as necessary to plan for a transaction.
6. We may disclose Personal Information where we believe doing so is necessary to protect our business, our employees, our rights and property, or the rights, property and safety of others.  For example, we may disclose Personal Information (i) to prevent, detect, investigate and respond to fraud, unauthorized activities and access, illegal activities, and misuse of the Nike premises, systems and networks, and (ii) in situations involving potential threats to the health, safety or legal rights of any person or third party. We may also disclose information, including Personal Information, related to litigation and other legal claims or proceedings in which we are involved, as well as for our internal accounting, auditing, compliance, recordkeeping, and legal functions.
7. We may disclose or make available your Personal Information to third-party platforms and providers that we use to provide or make available certain features or portions of our resources, tools, systems and networks.

## 5. Security and Governance of Personal information

1. Nike implements physical, technical and administrative security measures that are intended to protect your Personal Information. Please see Nike’s [Information Security Program(“NISP”)](http://nisp.nike.com/) for more information.
2. We also implement access controls to help ensure that access to Personal Information is limited to Nike personnel who need to have access to perform their duties. Please see the Enterprise Data Access Policy for more information.

## 6. Retention of Personal information

We will retain the Personal Information we collect for as long as reasonably necessary to support our ongoing legitimate business needs and to carry out the purposes described in this Policy or as otherwise required by applicable law. Generally, this means your Personal Information will be retained until the end of your employment or work relationship with us plus a reasonable period of time thereafter as required (1) to effectuate termination of our relationship, (2) by applicable law or regulation, (3) to respond to employment or work-related inquiries or issues, or (4) to provide you with ongoing pensions or other benefits. If you continue to receive benefits from us after the end of your employment, we will continue to manage and process your Personal Information as described above. For more information about Nike's data retention practices, including in respect of employee records, please refer to Nike's [Records Retention Policy.](https://cao-org.nike.com/information-governance/policy/)

## 7. Updates to this Policy

We may change, update, or modify this Policy from time to time. If we make any changes to this Policy that materially affect our practices regarding the Personal Information we have previously collected from you, we will endeavor to provide you with notice in advance of such change, such as by contacting you at the email address we have on record.

## 8. Contact Information

If you have questions regarding this Policy, please contact your local HR manager. You may also contact Nike’s Privacy Office or Data Protection Officer by emailing [privacy.office@nike.com](mailto:privacy.office@nike.com).

## **Additional Information for California Residents**

**If you reside in California, the following additional California-specific provisions apply to the processing of your Personal Information:**

This California Employee Privacy Policy and Notice at Collection (“Employee Notice”) provides specific information for residents of California who work for Nike. This Employee Notice is intended to satisfy our applicable notice requirements under the California Consumer Privacy Act (“CCPA”) (Cal Civ. Code § 1798.100 et seq.), as amended by the California Privacy Rights Act (“CPRA”).

Personal Information for purposes of this Employee Notice does not include:

·       Publicly available information that is lawfully made available from federal government records;

·       Information we have a reasonable basis to believe is lawfully made available to the general public by you, by widely-distributed media, or by a person to whom you have disclosed the information and not restricted it to a specific audience;

·       Information that is deidentified or aggregated;

·       Protected Health Information that is governed by the Health Insurance Portability and Accountability Act ("HIPAA"); and

·       Information we receive from consumer reporting agencies that are subject to the Fair Credit Reporting Act ("FCRA") (e.g., information contained in background check reports we obtain as part of our hiring process).

**1.         Information We Collect**

As further discussed in “Types of Personal Information We Collect and How We Use Them” above, the table below identifies, generally, the categories of Personal Information about you that we may collect, and that we have collected in the previous 12 months, about California residents in their capacity as Nike employees. Some Personal Information included in the categories below may overlap with other categories.

|  |  |  |  |
| --- | --- | --- | --- |
| **Categories of Personal Information** | **Categories of Sources** | **Disclosed for a Business or Commercial Purpose** | **Have we Sold or Shared in the Past 12 Months?** |
| **Identifiers**   * Including name, former last name, suffix, alias, address, email address, date of birth, unique personal identifier, online identifier, Internet Protocol (IP) address, social security number, driver’s license number, passport number, or other similar identifiers. | * From you directly. * From other businesses (e.g., benefits providers). * From publicly available sources such as company websites or professional networking sites. * From professional references. | Yes | No |
| **Characteristics of protected classifications**   * Including age, race, ancestry, national origin, citizenship, marital status, pregnancy, medical condition, physical or mental disability, sex, veteran or military status and other characteristics of protected classifications under California or federal law. | * From you directly. * From other businesses (e.g., benefits providers). | Yes | No |
| **Professional or employment-related information**   * Including current and former employer(s), employee ID, office phone number, company cell number, work email, employment history, qualifications, professional memberships, licensing, disciplinary record, or any other related information. | * From you directly. * From publicly available sources such as company websites or professional networking sites. * From professional references. | Yes | No |
| **Internet or other electronic network activity information**   * Including browsing history, interactions with our systems, networks and applications. | * From you directly. * Through our websites, mobile apps, systems, networks, and online services. * From third-party service providers. | Yes | No |
| **General geolocation data**   * Location information about a particular individual or device. | * From you directly. * Through our websites, mobile apps, and online services. * From third-party service providers. | Yes | No |
| **Audio, visual, or similar information**   * Such as audio, electronic, visual, or similar information, including information collected via call recordings, recorded meetings, videos, photographs, and CCTV footage to secure our offices and premises. | * From you directly. * From third-party service providers. | Yes | No |
| **Education information**   * Including education records, including schools attended, degrees awarded, dates of attendance, grades, transcripts, student disciplinary records, or any other related information. * Information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99). | * From you directly. * From educational institutions or providers of educational or professional certification information. | Yes | No |
| **Sensitive Personal Information**   * Such as social security number, driver’s license number, precise geolocation information derived from a Nike device, state identification card, passport number, racial or ethnic origin, medical conditions, physical or mental disability, sexual orientation, Nike account login credentials, financial account information, and the content of your emails and other electronic messages sent using a Nike account, device, app, platform, or system. | * From you directly. * Through our websites, mobile apps, and online services. | Yes | No |
| **Profiles and inferences**   * Inferences drawn from any of the information identified above to create a profile reflecting an individual’s preferences, characteristics, behavior or attitudes. | * From you directly. | Yes | No |

**2.         Sales and Sharing of Personal Information**

We do not sell or share, as those terms are defined under the CCPA, Personal Information or sensitive Personal Information about employees, including those who we know are under 16 years old.

**3.         How We Use Information**

Generally, we may use the categories of Personal Information described above for the following business or commercial purposes (and any directly related purposes), as further described in "Types of Personal Information We Collect and How We Use Them" above:

* Onboarding
* Human resources management
* Safety and security
* Offboarding
* Voluntary programs
* Sensitive data processing
* Compliance with legal obligations
* Defending and protecting rights
* Mergers, acquisitions and other business transactions
* Auditing, accounting, reporting and corporate governance
* Other legitimate business purposes

**Use of Sensitive Personal Information**.  Our collection, use and disclosure of sensitive Personal Information is generally limited to what is reasonable and proportionate for the following purposes:

* To comply with our legal, regulatory and reporting obligations;
* To make reasonable accommodations where necessary;
* To verify the information you provide to us;
* As otherwise necessary to carry out our functions as an employer;
* In support of our equal opportunity and diversity and inclusion efforts (on a voluntary basis);
* Where necessary to protect the health and safety of an individual; and
* To protect and take action against malicious, deceptive, fraudulent, or illegal actions, security incidents.

We do not use or disclose employee sensitive Personal Information for purposes except as described herein (and as permitted pursuant to Cal. Code Regs. tit. 11, § 7027(m) (2022)).

**4.         Disclosures of Personal Information**

As further described in “Disclosures of Personal Information” above, we may disclose or have in the previous 12 months disclosed the above categories of Personal Information for a business purpose to the following categories of recipients on a need-to-know basis:

* Our personnel, including personnel of our affiliates;
* Service providers and vendors that act on our behalf to process Personal Information for administrative, management, or business purposes and to assist us in providing our products and services.  These include accountants, law firms and legal service providers, tax or financial professionals, payroll and benefits providers, relocation companies, pension and insurance companies, human resources specialists, consultants, contractors, and IT support and storage providers;
* Third-party researchers and publishers;
* Governmental bodies, law enforcement, or regulatory authorities where required by applicable law, in the context of lawful requests, court orders, legal proceedings or investigations;
* Potential or prospective buyers, sellers, lenders and their respective affiliates, agents, advisers, representatives, employees, and officers in event of corporate transactions such as a financing, merger, acquisition, takeover, bankruptcy, amalgamation, reorganization or other sale or disposal of assets or interests; and
* Third-party platforms and providers.

If required under the CCPA, we will obtain your consent prior to disclosing your Personal Information.

**5.         Data Retention**

We will retain the Personal Information we collect for as long as reasonably necessary to support our ongoing legitimate business needs and to carry out the purposes described in this Policy or as otherwise required by applicable law. Generally, this means your Personal Information will be retained until the end of your employment or work relationship with us plus a reasonable period of time thereafter as required (1) to effectuate termination of our relationship, (2) by applicable law or regulation, (3) to respond to employment or work-related inquiries or issues, or (4) to provide you with ongoing pensions or other benefits. If you continue to receive benefits from us after the end of your employment, we will continue to manage and process your Personal Information as described above. For more information about Nike's data retention practices, including in respect of employee records, please refer to Nike's [Records Retention Policy.](https://cao-org.nike.com/information-governance/policy/)

**6.         Your California Privacy Rights**

Under the CCPA, employees who reside in California have the following rights (subject to certain conditions, limitations and exceptions) regarding the Personal Information we collect. Importantly, these rights do not affect other rights you may have under the California Labor Code.

* **Right to Know/Request Access**. The right to know what Personal Information we have collected about you, including the categories of Personal Information, the categories of sources from which the Personal Information is collected, the business or commercial purpose for collecting, selling, or sharing Personal Information, the categories of third parties to whom we disclose Personal Information, and the specific pieces of Personal Information we have collected about you.
* **Right to Correct**. Subject to certain restrictions, you have the right to request that we correct inaccuracies in your Personal Information.
* **Right to Delete**. Subject to certain conditions and exceptions, you have the right to request deletion of your Personal Information that we have collected about you.
* **Right to Opt-Out**. You have the right to opt-out of “sales” and “sharing” of your Personal Information, as those terms are defined under the CCPA. However, we do not sell or share our employees’ Personal Information, so there is no need to exercise these rights.
* **Right to Limit Use and Disclosure**. We do not engage in uses or disclosures of Personal Information that would trigger the right to limit use of sensitive Personal Information under the CCPA.
* **Right to Non-Discrimination**. We will not discriminate against you for exercising any of the rights described in this section.

**Exercising Your California Privacy Rights**

Employees who are California residents may submit a request to exercise their CCPA rights via the methods described below:

* **Email** us at [hrdirect.americas@nike.com](mailto:hrdirect.americas@nike.com)
* **Call** us at 888-360-6453

We will take steps to verify your request by  providing you with instructions to authenticate your identity through our corporate systems and and/or matching the information provided by you with the information we have in our systems. We will process your request based upon the Personal Information in our records that is linked or reasonably linkable to the information provided in your request. In some cases, we may request additional information in order to verify your request or where necessary to process your request. If we are unable to adequately verify a request, we will notify the requestor.

Authorized agents may initiate a request on behalf of another individual using the same methods described above. Authorized agents will be required to provide proof of their authorization, and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.  You may also provide us with a signed and dated power of attorney naming the authorized agent as your representative.

We reserve the right to reject (1) authorized agents who have not fulfilled the above requirements, or (2) automated rights requests where we have reason to believe the security of the requestor’s Personal Information may be at risk.

**Response Timing and Format.**

We endeavor to respond to a consumer request within 45 days of receipt. If we require more time (up to 90 days total), we will inform you of the reason and extension period in writing.

If we cannot respond to your request, either fully or partially, we will also explain our reasons. For data access requests, we will deliver the data in a readily, useable format.

**Rights Under California Shine the Light Law**.  We do not share Personal Information of employees with third parties for their own direct marketing use.

**ACCEPTABLE USE POLICY:   
ELECTRONIC COMMUNICATIONS AND DEVICES**

Nike, Inc., and its subsidiaries and affiliates (including your employer, “Nike”) provide their employees with devices and electronic communication tools and systems for use in supporting business activities. These systems include Nike-owned hardware or Nike-licensed and approved software including company servers, company email accounts, applications, programs, company shared drives or file shares, message boards, instant messaging systems, blogs, internet channels, company cloud storage locations and various other systems (“Nike Systems”).

The following Policy provides continued support for employees to ‘Keep it Tight,’ and also helps to ensure that all electronic communication using Nike Systems is appropriate, professional, and legally compliant.

**1. NIKE May Access NIke Systems and Monitor Your Communications**

1.1. Subject to this Policy and any local Policy addendums applicable in your location, Nike monitors employee access to Nike Systems by way of automated tools that may scan, filter and record activities and communications on Nike Systems (even when employees are absent and off campus), to protect against unauthorized access and use of Nike Systems and any company-related information held in electronic form. This includes company emails and other communications, documents, data, databases, images, graphics, photos and other materials, which may include, but is not limited to, proprietary, confidential or personal information of Nike, its clients, consumers, suppliers, partners or other third parties ("Nike Material").  There should be no expectation of privacy in anything employees communicate, store or access when they access and use Nike Systems or Nike Material, which are considered Nike’s property, subject only to mandatory provisions of local law.  Nike has full authority to manage the Nike Systems and Nike Material, including the installation of software that tracks and records device and data activity in the Nike Systems.

1.2. Nike Systems are provided to support Nike business and to give you the right tools and resources for performing your job.  Subject to any local Policy addendum or monitoring notice, which would override the terms in this Policy, and as permissible by applicable law, incidental and occasional non-business use of the Nike Systems is permitted within Nike.  But any use of the Nike Systems and the content of any materials communicated on Nike Systems, including personal materials and information, may be viewed and recorded by Nike for legitimate business purposes, including the following: ensuring security of Nike Systems and all data contained or transmitted therein, in particular Nike Material; securing proprietary information; preventing or mitigating the misappropriation of Nike Material; and verifying use patterns and activity on Nike Systems in order to anticipate, detect, thwart and evidence attacks on and infiltration of Nike Systems.  To the extent allowed under applicable law, employees’ personal information, if any, may also be processed for investigations and legal proceedings if the monitoring reveals unlawful acts or violations of Nike policies. Personal information will be accessed exclusively by persons authorized by Nike and any processing of your personal information will be performed in a manner intended to limit the impact on employee’s privacy and kept for the time necessary to achieve the purposes outlined above.

1.3. Where there is a justified suspicion of any threat, security violation or misappropriation in relation to Nike Systems or Nike Material, Nike may engage in supplemental monitoring, viewing or recording of any activity in the Nike Systems. Information relating to and produced by such viewing and recording activities may be disclosed, without notice or other restrictions, to other Nike group entities and to third party providers and law enforcement, which may be located outside the country of employment, for any of the purposes set forth in this Policy or to comply with applicable law. Subject to any Nike local monitoring policy or notice, and as permissible by applicable law, Nike reserves the right to access at any time the Nike Systems using automated tools or by manual review, to monitor data and messages within the Nike Systems, and to read, reject or remove any message (including attachments) composed, sent or received, for the purposes set forth in this Policy or to comply with applicable law. Nike reserves the right to limit and/or terminate access to Nike Systems at any time, as a result of non-compliance with this Policy, or for any other reason consistent with the purposes set forth in this Policy; such right may be further described in other Nike policies or employment contracts, if applicable.

1.4. Nike Systems are not designed for personal employee use.  Subject to this Policy and any local Policy addendums applicable in your location,employees who do make incidental and occasional personal use of Nike Systems should file personal materials in a separate folder clearly marked as such (by marking or naming the folder “PERSONAL”).  Consistent with and subject to local law and process, Nike reserves the right to access material stored in that location on a Nike device, despite its being marked as Personal, to the extent doing so is necessary to protect Nike Systems and Nike Material. Consistent with and subject to local law and process, any personal materials stored in Nike Systems may be used against you to the fullest extent permissible under applicable law, including to justify termination or in the context of litigation.

1.5. To protect Nike Systems and Nike Material, Nike may remotely wipe Nike-owned devices at any time.  When leaving Nike, employees must return their Nike-owned device(s) and all Nike Material to Nike.  Employees’ access to Nike Materials, including company email, will be terminated when the employee leaves the company.  It is the employee's obligation to remove or retrieve any personal materials that may exist on their Nike-owned devices, and while Nike will seek to provide opportunity for employees to remove personal materials on Nike-owned devices employees may not be guaranteed an opportunity to obtain copies of all personal materials on those devices. Nike’s right to view, record, access and monitor Nike Systems and Nike Material remains enforceable even after you leave Nike and surrender the device to Nike. Failure to return Nike devices to Nike can result in potential legal action against the former employee.

**2. Keep NIKE's Secrets**

2.1. Nike business may only be conducted on Nike Systems.  Employees may not use personal communications channels, such as personal email accounts, to conduct Nike work.  Employees may not forward any Nike Materials to a personal email account or non-approved external file sharing programs without a legitimate business need and pre-approval.

2.2. All employees are responsible for ensuring that Nike's non-public, proprietary or confidential information does not enter the public domain (for example, through electronic transmissions). Employees are responsible for securing any Nike Material in their possession.  All employees are also responsible for complying with the terms of any confidentiality and proprietary agreements they have signed, or similar provisions in employment agreements or other Nike policies, including Nike’s Confidential Information and Trade Secret Policy.

2.3. Nike's proprietary and confidential information includes, but is not limited to, any information, data, ideas, plans, strategies, concepts or proposals relating to the following:

* inventions, patents, prototypes, and unreleased products;
* marketing, sales, promotional plans and ideas, and customer information;
* production data, futures orders, and forecasts;
* corporate matters governed by government regulations (including SEC regulations), such as earnings, sales and forecasts;
* communications with company lawyers or documents marked confidential;
* personal information of consumers, elite athletes, research subjects, Nike employees and independent contractors, customers and suppliers/vendors; or
* anything else which, in the wrong hands, could be an advantage to Nike's competitors or could put Nike at a competitive disadvantage.

2.4. If you have a question as to whether information is considered proprietary or confidential, be sure to talk with your manager before taking any next steps. In some cases, protection of confidential data is a legal requirement, not just a company policy. Legal requirements vary by country and employees should check with Nike's legal department to identify relevant local legal requirements.

2.5. Use the most secure communication method commercially available to transfer Nike's proprietary or confidential information, being mindful that Nike's private network and Nike-provided tools are always preferable to the Internet. Use Nike-provided email accounts, approved secure file transfer services, or approved messaging services to conduct Nike business; personal email accounts such as Gmail or Yahoo, and unapproved file transfer or messaging services, must not be used.  Nike Material, especially proprietary or confidential information, may not be shared except in the normal course of business and consistent with Nike policies.

**3. Make Sure Your Communications are Appropriate and Professional**

3.1. Do not use words, phrases or symbols in any electronic communications – either internal Nike communications or external business communications – that may be viewed by diverse audiences as inappropriate, offensive, or defamatory. Carefully review the content of any communications prior to publishing or distributing and consider the intended and unintended audiences (as content could be shared beyond the original audience). Consider whether the content, if shared publicly or subpoenaed, would be damaging or embarrassing to either you or Nike. Nike's anti-harassment and anti-discrimination policies and any similar provisions in company handbooks, work rules, internal regulations or your employment agreement apply to written as well as verbal internal and external business communication. Subject to any Nike local monitoring policy or notice, and as permissible by applicable law, Nike may review communications to determine whether any Nike policy is violated, and will take appropriate steps to remedy any inappropriate behavior.

**4. Internal blogs and other Internal communication**

4.1. When developing an internal blog or other communication, remember that all Nike policies apply, including this Policy and [the Matter of Respect Policy](https://nikehr.nike.com/node/15978). If your blog or other communication contains links to other content outside your control (like an external website), be sure to first review all the links associated with the content to ensure that it is appropriate.

**5. Social Media Policy**

5.1. Use of social media platforms such as Facebook, Twitter, LinkedIn and others is addressed in [Nike’s Policy for Communication on External Websites and Social Media Platforms](https://nikehr.nike.com/node/471).

**6. Respect Copyrights and Other Material Owned by Third Parties**

6.1. Loading, sharing and maintaining unlicensed music, movies, software, or other similar items owned by third parties in Nike Systems is prohibited.

**7. Retention oF INFORMATION**

7.1. Nike will retain business records and information (which may include company email) for a specific retention period, depending on the type of record. There may also be laws and regulations that require Nike to retain certain records for a period of time, and it is Nike's policy to comply with them. At the expiration of the appropriate retention time, the information will be deleted or archived in accordance with applicable law. See the [Record Retention Policy and Schedule](https://nikehr.nike.com/node/366) for more information about appropriate retention periods.

**8. Improper Use**

8.1. Improper use of the Nike Systems or Nike Material, as outlined in the applicable Nike policies or in employment contracts, if applicable, may result in limitation or revocation of your electronic access privileges as well as corrective action, up to and including termination. Activities that may constitute improper use include, but are not limited to, the following:

* sending Nike Material to anyone not entitled to know or possess it;
* accessing Nike Material for non-business uses;
* sending or retrieving sexually explicit or offensive messages, cartoons or jokes, ethnic slurs, racial epithets or any other statement or image that might be construed as harassment, defamation or libel using Nike Systems or when conducting Nike business;
* conducting Nike business outside Nike Systems (for example, with non-Nike-provided or approved electronic communications systems);
* accessing Nike Material (1) through a device that is not provided by Nike, or (2) outside Nike-approved secure access methods, including but not limited to: mobile device management systems, virtual desktop infrastructure, VPN connections, or Nike-provided secure applications;
* operating a personal business using Nike Systems or using Nike Systems or Nike Material for other commercial purposes unrelated to Nike’s;
* making excessive or unreasonable personal use of Nike Systems, including use that interferes with your work performance or uses more than a trivial amount of resources;
* sending unsolicited or unwanted personal views on social, political, religious or other non-business-related matters using Nike Systems;
* engaging in unlawful activities, including sending or receiving copyrighted materials in violation of copyright laws or license agreements using Nike Systems;
* automatic forwarding Nike individual user email to any external address;
* engaging in personal business, profit-making activities, or personal activities that incur additional costs to Nike or interfere with an employee's work performance;
* creating and installing any virus, worm, Trojan Horse, or any other type of electronic file that might have the ability to harmfully affect another user or system or gather personal or business information without approval;
* sending chain letters, non-business-related attachments, advertisements, greetings and broadcast messages (including computer virus warnings) using Nike Systems;
* sharing of your password(s) for Nike Systems with anyone, both external and internal to Nike;
* allowing someone to access Nike Systems or Nike Material while leveraging the rights and permissions of your Nike account(s);
* knowingly accepting, transmitting or distributing unsolicited bulk email, or harvesting or collection of email addresses from Nike Systems for the purpose of sending unsolicited email; or
* any other violation of Nike policy or applicable law.

**9. PROTECTING YOUR PERSONAL INFORMATION**

9.1. Any personal information Nike collects and processes in furtherance of this Policy will be processed and stored for the purposes and by the recipients described in this Policy and in compliance with Nike’s Employee Privacy Policy, to the extent such a policy is in effect in your location.

9.2. Nike reserves the right to modify or to rescind this Policy at any time, consistent with applicable law. Also, this Policy is subject to and may be superseded by any local policies that a Nike company may adopt. For example, retail employees should check with Retail Store Operations Policy which may have different or additional requirements.

9.3. It is important for employees to understand that this Policy should not interfere with any rights protected under local or country law, including, where applicable, employees' rights to access personal data and discuss their terms and conditions of employment.

9.4. Employees who have questions or other inquiries about anything covered in this Policy may contact Nike Human Resources through HR Direct.