	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

IT038 - BIOMETRICS PRIVACY, RETENTION, AND DESTRUCTION POLICY

Purpose:

The Company collects the Biometric Information for the following purposes: for employee and contractor onboarding, scheduling, punching in and out, building access, time clocks, accuracy in recording time entries, scheduling, security, and safety. The Company also discloses the Biometric Information to its vendors and service providers and any of their affiliates, subcontractors, resellers or successors (collectively, “Service Providers”) who utilize the Biometric Information in support of these same purposes.

The Company and Service Providers will not sell, lease, trade, or otherwise profit from employees or contractors’ Biometric Information provided. However, the Company’s Service Providers may be paid for products or services used by the Company that utilize such Biometric Information.

Definitions:

Reference the IT Policy Glossary


Scope:

Employees and contractors located in the United States and Canada.

Policy:

Background/Information:

Gordon Food Service, Inc. and Gordon Food Service Canada Ltd. and its affiliates and subsidiaries (the “Company”) may collect certain biometric data from employees and contractors located in the United States and Canada. This Biometric Privacy, Retention, and Destruction Policy (“Biometric Policy”) explains what information the Company may collect, how this information may be used, and how it is stored,

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

safeguarded, retained, and disposed of. This Biometric Policy also provides details regarding the alternatives that are available to employees and contractors who do not wish to provide their Biometric Information.


For purposes of this Biometric Policy, “Biometric Information” means personal information stored by the Company regarding an individual’s physical characteristics that can be used to identify a person, such as fingerprints, voiceprints, photos, facial shape, scan of hand or face geometry, or mathematical representations of hand or face geometry, and as defined by applicable State and local laws. Biometric Information includes “biometric identifiers” and “biometric information” and as defined by applicable state or local laws. The Company may utilize biometric technology and collect the following Biometric Information:

- Fingerprints and facial images although the finger and face scan timekeeping devices do not store this information. When using those timekeeping devices, the device’s enrollment process performs a set of measurements of the finger or face scan. The data is converted at the devices prior to storage by a proprietary algorithm into mathematical representations (encoding), known as a template, that cannot be reverse-engineered into an individual’s actual fingerprint or facial geometry.
- Other time keeping devices may take your picture and identify you with its face-matching system.

Procedure:

To the extent that the Company and its Service Providers collect, capture, or otherwise obtain Biometric Information relating to an employee or contractor, the Company shall first:

1. Inform the employee or contractor in writing that the Company and its Service Providers are collecting, capturing, or otherwise obtaining the employee or contractor’s Biometric Information and that the Company is providing such Biometric Information to its Service Providers;
2. Inform the employee or contractor in writing of the specific purpose and length of time for which the employee or contractor’s Biometric Information is being collected, stored, and used; and

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

- Receive a written electronic release signed by the employee or contractor (or his or her legally authorized representative) authorizing the Company, and its Service Providers to collect, store, and use the employee or contractor’s Biometric Information for the specific purposes disclosed by the Company, and for the Company to provide such Biometric Information to its Service Providers. For certain timekeeping devices, the written electronic release will also be obtained at the timekeeping device itself. The employee or contractor is free to decline to provide Biometric Information without any adverse consequence by the Company and, if they consent, later may revoke this consent at any time by notifying the Company in writing or through the Company’s biometric technology where available.


Responsibilities:

Disclosure

The Company stores all Biometric Information in accordance with applicable standards and laws. The Company will not sell, lease, trade, or otherwise profit from an employee or contractor’s Biometric Information.

The Company will only disclose or disseminate Biometric Information in accordance with applicable law. The Company will not disclose or disseminate Biometric Information to anyone including its Service Providers without/unless:

- First obtaining written employee or contractor consent to such disclosure or dissemination;
- The disclosed data completes a financial transaction requested or authorized by the employee or contractor;
- Disclosure is required by state or federal law or municipal ordinance; or
- Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

Biometric Information may therefore be held outside the region in which it was collected. Biometric Information processed and stored in another jurisdiction may be subject to disclosure or access requests by the governments, courts or law enforcement or regulatory agencies in that jurisdiction, according to its laws.

Record Retention Requirement:

Retention Schedule

The Company shall retain Biometric Information only until, and shall request that its Service Providers permanently destroy such data when, the first of the following occurs:


1. The initial purpose for collecting or obtaining such Biometric Information has been satisfied, such as the termination of the employee or contractor’s relationship with the Company; or
2. Within 1 year of the employee or contractor’s last interaction with the Company.

Biometric Information will be deleted from the Company’s Biometric Software systems promptly after an employee or contractor’s relationship with the Company ceases.

In no situation will Biometric Information be retained for more than one year after an employee or contractor’s last interaction with the Company, unless otherwise required by law.

Data Storage

Biometric Information will be stored, transmitted, and protected using a reasonable standard of care for the Company’s industry, in a manner that is the same as or that exceeds the standards of care used to protect other confidential information held by the Company. This includes, among other things, restricting access to Biometric Information to authorized Company employees, contractors or Service Providers who have a business need to access the information, and using reasonable technological means to prevent unauthorized access to the information. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

individual’s account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver’s license numbers and social security numbers.

Your Rights and Options Concerning Your Biometric Information:

Data Subject Rights

Data Subject Rights

Under certain circumstances and subject to applicable State and local laws, supported by a written request and proof of identification, you may consult the Biometric Information that we have collected, used or communicated, and/or ask that it be corrected, and/or withdraw your consent to our disclosure or use of Biometric Information collected.

Options


If an employee or contractors refuses to give their consent or withdraws their consent to the collection, use or retention of Biometric Information, the Company has provided the following alternative system: employees may use their GFS employee identification badges or their badge number for identification.

Document Review and Approval Requirements:

A copy of this policy will be made publicly available at www.GFS.com.
The Company will update this policy if it begins collecting Biometric Information for any other purposes.
The Company reserves the right to amend this policy at any time.

Attachments/Appendices

- APPENDIX A - Notice and Consent for Use with Employees.
- APPENDIX B - UKG / Third-Party App (as applicable) Timeclocks Notice and Consent


	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

**Notice and Written Consent/Release Regarding
Data Processing of Biometric Information and Identifiers.**

This notice and written consent/release (“Notice”) is intended to describe the type of Biometric Information (defined below) that Gordon Food Service, Inc. Gordon Food Service Canada Ltd. and its affiliates and subsidiaries (“GFS”) collects from you, why it is being collected, how it is stored, used, and destroyed, as well as where you can find more information about GFS’s Biometric Privacy, Retention and Destruction Policy (“Biometric Policy”). If you have not fully read GFS’s Biometric Policy, please do so first before returning to this Notice. GFS’s Biometric Policy is attached as Exhibit A and is also available on our internal network linked here for the [United States](#) and here for [Canada](#) and available on the web at gfs.com or gfs.ca.

For purposes of this Notice, Biometric Information means personal information stored by the Company regarding an individual’s physical characteristics that can be used to identify a person, such as fingerprints, voiceprints, photos, facial shape, scan of hand or face geometry, or mathematical representations of hand or face geometry, and as defined by applicable State and local laws. Biometric Information includes “biometric identifiers” and “biometric information” as defined by applicable state or local laws. The Company may utilize biometric technology and collect the following Biometric Information:


- Fingerprints and facial images although the finger and face scan timekeeping devices do not store this information. When using those timekeeping devices, the device’s enrollment process performs a set of measurements of the finger or face scan. The data is converted at the devices prior to storage by a proprietary algorithm into mathematical representations (encoding), known as a template, that cannot be reverse engineered into an individual’s actual fingerprint or facial geometry.
- Other time keeping devices may take your picture and identify you with its face matching system.

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

By signing this Notice, you are indicating that you give informed consent to GFS’s processing of your Biometric Information as it is outlined in this Notice and GFS’s Biometric Policy. You are free to decline to provide Biometric Information without any adverse consequence by GFS and, you later may revoke this consent at any time by notifying GFS in writing. You will be notified in writing before any changes to this Notice or the Biometric Policy are implemented.

If an employee or contractor refuses to give their consent or withdraws their consent to the collection, use or retention of Biometric Information, the Company has provided the following alternative system: employees may use their GFS employee identification badges or their badge number for identification.

1. What is GFS's specific purpose for collecting, storing and using my Biometric Information?
 - a. GFS collects, uses, stores the Biometric Information identified above from you for the following purposes: workforce management systems (for example, employee onboarding, scheduling, punching in and out), building access, time clocks, to ensure accuracy in recording time entries, scheduling, security, and safety. Our vendors and service providers whose technology supports this activity also receive and store this information, which includes UKG Inc., or an affiliate, vendor, subsidiary, or related company of UKG, Inc., including Kronos and any of their subcontractors, resellers or successors (collectively “Service Providers”).
2. How will my Biometric Information be collected?
 - a. The Biometric Information will be collected in the form of photos and/or scans of employee or contractor’s fingers or faces, to verify that they are “clocking in” or “clocking out.”
3. How long will my Biometric Information be stored?
 - a. GFS shall retain Biometric Information only until, and shall permanently destroy such data when, the first of the following occurs:
 - i. The initial purpose for collecting or obtaining such Biometric Information has been satisfied, such as when your employment with GFS ends; or
 - ii. Within one (1) year of your last interaction with the Company.


	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

GFS shall direct its Service Providers to permanently destroy the Biometric Information within this same retention schedule outlined immediately above.

4. How will GFS dispose of my information once it is no longer needed?
 - a. GFS will delete the Biometric Information at the device as set forth in Section 3(a) and 3(b) above and on any databases maintained by our Service Providers, subject to our internal policies, Record Retention Policy, applicable contracts, laws, and any active legal proceedings.
5. Will GFS disclose my Biometric Information to third parties or other jurisdictions?
 - a. Yes, we disclose your Biometric Information to our Service Providers including UKG and its service providers and when required by law. GFS will not disclose this information to any other third parties unless required by law. Note, your Biometric Information will be stored locally on the device and in servers located in the United States. While such information is outside of your jurisdiction of residence, it is subject to the laws of the jurisdiction in which it is held, and may be subject to disclosure to the governments, courts or law enforcement or regulatory agencies of such other jurisdiction, pursuant to local laws.
6. Where can I find GFS's Biometric Policy?
 - a. GFS's Biometric Policy is attached as Exhibit A and is also available on our internal network linked here for the [United States](#) and here for [Canada](#) and available on the web at gfs.com or gfs.ca. GFS's Biometric Policy contains additional details concerning GFS's collection, processing, and communication of your Biometric Information, including information concerning your rights, and how to exercise them.

EMPLOYEE/CONTRACTOR WRITTEN CONSENT/RELEASE & ACKNOWLEDGMENT OF THIS NOTICE AND GFS'S BIOMETRIC POLICY


I, _____, have read this Notice and GFS's Biometric Policy, and I consent to these documents and their terms. By signing, I acknowledge that I understand and expressly agree that my Biometric Information will be collected, stored, collected, used, disclosed, and destroyed pursuant to this Notice

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

and the GFS Biometric Policy. You are free to decline to provide Biometric Information without any adverse consequence by GFS and, you later may revoke this consent at any time by notifying GFS in writing.

Signed: _____

Dated: _____

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

APPENDIX B - UKG / Third Party App (as applicable) Timeclocks Notice and Consent


UKG Face Scan Timekeeping Device Notice and Consent

I agree and intend to use my employer’s timeclock devices with a face camera and face scan software for timekeeping and attendance. I understand that the device will take a photograph of my face and uses data from it to create a template that is securely stored in the device and my employer’s timekeeping database during my employment. I understand that the face scan data and template may be considered biometric data, as defined in applicable laws. By clicking “Accept” below and completing enrollment, I confirm that I agree to my employer’s policy regarding biometric data retention, and destruction. Clicking “Accept” is my signature and Consent to the collection, capture, storage, access to, use, possession, dissemination, disclosure, re-disclosure, and hosting of any biometric data by my employer, UKG Inc. (or an affiliate, vendor, subsidiary, or related company of UKG, including Kronos) and any of their subcontractors, resellers or successors, consistent with my Consent and my employer’s Biometric policy. My Consent applies to each use of the face camera and face scan software, including past and future use. I acknowledge that I have reviewed my employer’s Biometric Privacy Policy and am aware of my own legal rights regarding data privacy, including, subject to applicable laws, my rights to access and/or rectify my personal information, as well as my right to withdraw my consent. I also acknowledge that my personal information may be stored outside of my jurisdiction of residence. I acknowledge that I am able to print and keep a copy of this notice at UKG.com/noticeandconsent.

ACCEPT/DECLINE

UKG Finger Scan Timekeeping Device Notice and Consent


I agree and intend to use my employer’s timeclock devices with a finger sensor for timekeeping and attendance. I understand that the sensor uses data from my finger scan and creates a template that is securely stored in the sensor and my employer’s timekeeping database, during my employment. I understand that finger scans and templates may be considered biometric data. By clicking “Accept” below and completing enrollment, I confirm that I agree to my employer’s policy regarding biometric data retention and destruction. Clicking “Accept” is my signature and Consent to the collection, capture,

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

storage, access to, use, possession, dissemination, disclosure, re-disclosure, and hosting of any biometric data by my employer, UKG Inc. (or an affiliate, vendor, subsidiary, or related company of UKG, including Kronos) and any of their subcontractors, resellers, or successors, consistent with my Consent and my employer’s Biometric Privacy Policy. My Consent applies to each use of the sensor, including past and future use. I acknowledge that I have reviewed my employer’s written Biometric policy and am aware of my own legal rights regarding data privacy, including, subject to applicable laws, my rights to access and/or rectify my personal information, as well as my right to withdraw my consent. I also acknowledge that my personal information may be stored outside of my jurisdiction of residence. I acknowledge that I am able to print and keep a copy of this notice at UKG.com/noticeandconsent.

ACCEPT/DECLINE

[END]

	Policy Name: Biometrics Privacy, Retention, and Destruction Policy	
	Policy Owner: Chief Legal & Risk Officer; Enterprise Information Security Officer	Date of Last Revision: N/A Date Created: 11/01/2023
	Approved By: Chief Legal & Risk Officer; Enterprise Information Security Officer	Type: Complete Revision: () Partial Revision: () New: (X)

Revision History:

2023-11-01: This policy is new and incorporates policy statements previously published in the Gordon Food Service Employee Code of Conduct, Personal Information Protection.