NCCO PRIVACY POLICY

Effective Date: October 1, 2026

Introduction

National Checking Company, doing business as NCCO, together with the NCCO affiliate identified as the provider of the applicable website, product, service, account, order form, or checkout process (collectively, **"NCCO," "we," "us,"** or **"our"**), respects your privacy. This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information and describes the choices and rights that may be available to you.

1. Scope

This Privacy Policy applies to personal information that we collect through:

- https://www.ncco.group/;
- https://www.ncco.com/;
- https://store.ncco.com/;
- https://www.datecodegenie.com/;
- https://alwaysfoodsafe.com/;
- https://www.dotit.com/;
- https://www.orderpads.com/;
- any current or future NCCO website, online store, mobile application, account portal, or online service that links to this Privacy Policy (collectively, the **"Services"**);
- orders, enrollments, support requests, marketing communications, and other interactions conducted through the Services.

This Privacy Policy does not apply to:

- workforce or job-applicant personal information;
- business-contact information subject to B2B contracts and relationships;

- third-party websites, applications, platforms, payment processors, or services that have their own privacy notices; or
- information NCCO processes solely on behalf of a business customer where NCCO acts as that customer's service provider or processor, except as otherwise stated in an applicable agreement or notice.

The NCCO entity that is the controller of your personal information is the entity identified in the applicable order form, account terms, checkout flow, product terms, or other transaction documentation. If no entity is identified, the controller is National Checking Company, 899 Montreal Circle, St. Paul, Minnesota 55102.

PLEASE READ THIS POLICY CAREFULLY TO UNDERSTAND OUR POLICIES AND PRACTICES REGARDING YOUR INFORMATION AND HOW WE WILL TREAT IT. IF YOU DO NOT AGREE WITH OUR POLICIES AND PRACTICES, YOUR CHOICE IS NOT TO USE OUR WEBSITES OR SERVICES.

2. Personal Information We Collect

The personal information we collect depends on how you interact with us, the Services you use, and the choices you make, and may include the following categories of personal information:

System		Data	Collect?	Notes
A. E-commerce				
	Real Name	Yes		
	Password	Sometimes	Some systems use only NCCO shared ecosystem logins described below in (C); others store their own local password.	
	Email	Yes		
	Physical Address	Sometimes	In general, our sales are usually business-to-business, in which case addresses captured are usually business addresses. However, for AFS we have many individuals purchasing the course privately, and for other purchases we can't distinguish between personal addresses or business addresses provided.	
	Phone	Sometimes		
	Demographics	No		
	Birth Date	No		
	Tokenized Credit Card	Sometimes	We capture tokenized card information for physical product purchases; for Always Food Safe, we do not process or store this information. The tokenized card information cannot be used to obtain a real card number and cannot be reused in any other context.	
	Purchase History	Yes		
	Geolocation Data	No		
	Employment Information	Yes		
B. Marketing Websites		Ncco.com, ncco.co.uk, ncco.eu		

	Real Name	Yes	
	Password	No	
	Email	Yes	
	Physical Address	Yes	
	Phone	Yes	
	Demographics	No	
	Birth Date	No	
	Tokenized Credit Card	No	
	Purchase History	No	
	Geolocation Data	No	
	Employment Information	Yes	
C. Login/Organization Systems		Login.ncco.com	
	Real Name	Yes	
	Password	Yes	
	Email	Yes	
	Physical Address	Yes	Information collected is for businesses only, but the actual information may also be a person's personal information.
	Phone	Yes	As above
	Demographics	No	
	Birth Date	No	
	Tokenized Credit Card	No	
	Purchase History	No	
	Geolocation Data	No	
	Employment Information	Yes	Several systems record a person's association with a business (for example, being named as a user in the business' software account, use of a company-provided email address, or designation of a company name associated with an e-commerce order). This data may imply or reveal present employment status, but it is collected and used only to correctly provide services to or engage appropriately with the user or business involved and is not stored or represented as an employment history, except where otherwise noted.
D. DateCodeGenie		Datecodegenie.com	
	Real Name	Yes	
	Password	Sometimes	DCG can store credentials (username/password) which identify a unique user. This is moving to NCCO-ecosystem SSO per (C), but that is not fully deployed yet.
	Email	Sometimes	DCG users are in some cases required to supply an email address. The email the user provides may or may not be their personal address.
	Physical Address	Sometimes	DCG will typically store Administrator Contact information including business email, address, phone. This information could be personal but is used only for business purposes.
	Phone	Sometimes	
	Demographics	No	
	Birth Date	No	
	Tokenized Credit Card	No	
	Purchase History	No	
	Geolocation Data	No	
	Employment Information	No	
E. Salesforce		Salesforce.com	

	Real Name	Yes	
	Password	No	
	Email	Yes	Gathered for business and sales objectives; personal information may be provided for these purposes.
	Physical Address	Yes	As above
	Phone	Yes	As above
	Demographics	No	
	Birth Date	No	
	Tokenized Credit Card	No	
	Purchase History	No	
	Geolocation Data	No	
	Employment Information	No	
F. RightBytes		RightBytes.com	
	Real Name	Yes	
	Password	Sometimes	
	Email	Yes	
	Physical Address	Sometimes	DishPatch collects user information including address and phone number for the purpose of placing food orders.
	Phone	Sometimes	Certain systems collect phone numbers for PIN reset purposes and alert notification delivery.
	Demographics	No	
	Birth Date	No	
	Tokenized Credit Card	Yes	
	Purchase History	Yes	
	Geolocation Data	Yes	DishPatch allows the user to find nearby locations based on geolocation
	Employment Information	Yes	Several systems record a person's association with a business (for example, being named as a user in the business' software account, use of a company-provided email address, or designation of a company name associated with an e-commerce order). This data may imply or reveal present employment status, but it is collected and used only to correctly provide services to or engage appropriately with the user or business involved and is not stored or represented as an employment history, except where otherwise noted.
G. Internal Business Systems			
	Real Name	Yes	
	Password	No	
	Email	Yes	
	Physical Address	Sometimes	Always Food Safe needs to collect address and phone information for manager exam candidates as well as for proctor application purposes.
	Phone	Sometimes	In general, our sales are usually business-to-business. However, for AFS we have many individuals purchasing the course privately, and for other purchases we can't distinguish between personal addresses or business addresses provided.
	Demographics	No	
	Birth Date	No	
	Tokenized Credit Card	Yes	
	Purchase History	Yes	
	Geolocation Data	No	
	Employment Information	No	
H. Always Food Safe (except e-commerce)			

	Real Name	Yes	
	Password	No	
	Email	Yes	
	Physical Address	Sometimes	Always Food Safe needs to collect address and phone information for manager exam candidates as well as for proctor application purposes.
	Phone	Sometimes	As above
	Demographics	Yes	Always Food Safe needs to provide surveys including rough demographic categories (age range, for instance) in order to evaluate exam equitability and for accreditation purposes.
	Birth Date	Sometimes	Always Food Safe is required to collect a birth date for some state certification filing requirements. We collect this information only for that specific exam and state.
	Tokenized Credit Card	No	
	Purchase History	No	
	Geolocation Data	No	
	Employment Information	Sometimes	Proctor applications are required to include certain elements of employment history per accreditation directives

NCCO does not intentionally collect personal (non-work) contact information, sensitive personal data (such as health information, government identification numbers, or financial account details), or data from individuals under the age of 16.

Data is collected through the following means:

- Customer account creation and onboarding
- Execution of contracts and agreements
- Ongoing business communications and correspondence
- Customer support and service delivery interactions
- The Services provided
- Orders placed via e-commerce platforms, e.g. store.ncco.co.uk and store.ncco.eu.
- Information you provide us through any other means.

We may also collect information that does not directly identify you. If we combine it with personal information in manner that renders the combined data as personal information under applicable law, we will treat the combined information as personal information as required by law.

Sensitive Personal Information

We do not collect sensitive personal information through the Services. Financial information such as credit cards can be provided in connection with the Service. Credit card payments are handled by

through third party payment processors that maintain separate privacy policies for which they are solely responsible. We do not have access to raw credit card information and only exposed to tokenized non-identifiable representations of the original data. We do not use or disclose sensitive personal information to infer characteristics, traits, patterns, or behaviors about you.

3. Cookies and Similar Technologies

We and our service providers may use cookies, pixels, web beacons, SDKs, local storage, log files, and similar technologies to:

- operate, secure, and maintain the Services;
- remember settings and preferences;
- authenticate users and prevent fraud;
- measure traffic, performance, and engagement;
- understand how visitors use the Services; and
- where applicable and subject to your choices, support targeted advertising.

You can manage your cookie settings using the pop-up banner that appears in your browser. You can also manage cookies through your browser settings, although disabling certain cookies may affect the availability or functionality of the Services.

The Services may use cookies and similar tracking technologies for essential functionality and analytics purposes. A full description of NCCO's cookie practices, including opt-out options, is available in our Cookie Policy at https://www.ncco.com/privacy-policy-2/.

Where applicable law requires consent before we use non-essential cookies or similar technologies, we will obtain that consent before activating them.

4. How We Use Personal Information

We may use personal information as reasonably necessary and proportionate to:

- provide, operate, maintain, and improve the Services;
- create and administer accounts and subscriptions;

- process orders, payments, shipping, returns, training enrollments, certifications, and other transactions;
- provide customer service and respond to communications and requests;
- send transactional, service, security, account, legal, and—where permitted—marketing communications;
- personalize content and functionality;
- conduct analytics, testing, and quality assurance;
- protect the security, integrity, and availability of the Services and our systems;
- prevent, investigate, and respond to fraud, misuse, security incidents, and violations of our terms or law;
- comply with legal, regulatory, tax, accounting, contractual, and recordkeeping obligations;
- establish, exercise, or defend legal claims;
- to conduct internal reporting, analyze usage patterns, and improve our offerings using anonymized or aggregated analytics
- improvement and optimization or our business and Services; and
- conduct targeted advertising only where applicable, permitted by law, and subject to your choices and opt-out rights.

We may also use personal information for another purpose disclosed to you when we collect it or with your consent where consent is required by law.

5. How We Disclose Personal Information

We may disclose personal information to the following categories of recipients:

- **NCCO affiliates.** We may disclose personal information among NCCO-affiliated companies for the purposes described in this Privacy Policy.
- **Service providers and contractors.** We may disclose personal information to vendors that provide services for us in connection with the services we provide you, including hosting, cloud

infrastructure, e-commerce, payment processing, shipping, fulfillment, customer support, analytics, email delivery, security, professional services, learning-management, and IT providers.

- **Business and transaction partners.** We may disclose information where necessary to fulfill a transaction, provide a Service you request, or administer a business relationship.
- **Professional advisers.** We may disclose information to auditors, lawyers, accountants, insurers, and similar advisers when necessary for their services.
- **Corporate transaction participants.** We may disclose information in connection with an actual or contemplated merger, financing, acquisition, sale of assets, reorganization, bankruptcy, or other corporate transaction, subject to applicable law.
- **Government, legal, and safety recipients.** We may disclose information to government authorities, regulators, courts, law-enforcement agencies, or other parties where required or permitted by law, or where we reasonably believe disclosure is necessary to protect rights, safety, security, or property; prevent fraud; or enforce our agreements.
- **With your direction or consent.** We may disclose information when you ask or authorize us to do so.
- **Protective actions**. If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of Company, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.
- **Text Messaging**. We will not share your opt-in to an SMS campaign or communication with any third party for purposes unrelated to providing you with the services of that campaign or communication. We may share your personal data, including your SMS opt-in or consent status, with third parties that help us provide our messaging services, including but not limited to platform providers, phone companies, and any other vendors that assist us in the delivery of text messages.

We may disclose aggregated, deidentified, pseudonymized, or non-personal information without restriction, subject to applicable law.

6. Sales, Sharing, and Targeted Advertising

We do not sell or share personal information as those terms are defined under applicable U.S. privacy laws. We do not process personal information for targeted advertising.

We do not knowingly sell or share the personal information of individuals under 16 years of age.

7. Retention

We retain personal information only for as long as reasonably necessary and proportionate to fulfill the purposes described in this Privacy Policy, and to meet legal, accounting, tax, contractual, fraud-prevention, dispute-resolution, and recordkeeping requirements.

Our retention criteria include the nature and sensitivity of the information; the purposes for which it was collected; the duration of our relationship with you; applicable legal and contractual requirements; whether the information is needed to establish, exercise, or defend legal claims; and whether we can delete, aggregate, or deidentify the information.

We will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements.
To determine the appropriate retention period, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process it, and the applicable legal requirements.
By law, we are required to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax and accounting purposes.
Details of retention periods for different aspects of your personal data are available in our Retention Policy, a copy of which you may request by contacting our Data Privacy Manager using the details in Section 1.
In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

8. Your Privacy Choices and Rights

Depending on where you live, the applicable law that applies, and the nature of our processing, you may have the right to:

- confirm whether we process your personal information and obtain access to it;
- correct inaccuracies in your personal information;

- request deletion of personal information, subject to applicable exceptions;
- obtain a portable copy of certain personal information;
- opt out of the sale of personal information, sharing of personal information for cross-context behavioral advertising, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects;
- limit certain uses and disclosures of sensitive personal information, where applicable;
- request information about certain disclosures of personal information for direct-marketing purposes, where applicable;
- appeal our decision regarding a privacy-rights request; and
- not be discriminated against for exercising applicable privacy rights.

Submit a Request

To submit a privacy-rights request or email **privacymatters@NCCO.com**. Please state the right you wish to exercise and provide information sufficient for us to verify your identity and process your request.

Where permitted by law, an authorized agent may submit a request on your behalf. We may require proof of the agent's authority and may require you to verify your identity directly with us.

We will verify and respond to requests within the timeframe required by applicable law. We may deny, limit, or charge a fee for a request only where permitted by law. If we cannot fulfill a request, we will explain the basis for our decision to the extent required by law.

Appeals

If we deny your privacy-rights request, you may appeal by emailing **dataprivacy@ncco.com** with the subject line **"Privacy Rights Appeal"**. We will respond to your appeal within the time required by applicable law and, where required, provide information about additional recourse.

Universal Opt-Out Preference Signals

Where required by applicable law, we recognize and honor browser-based universal opt-out preference signals, such as Global Privacy Control, for processing that constitutes a sale, sharing, or

targeted advertising. A preference signal generally applies to the browser or device from which it is transmitted. We may associate the signal with your account only where legally permitted and technically supported.

Marketing Communications

You may opt out of marketing emails by using the unsubscribe link in the email. Your opt-out will not affect transactional, order-related, account, security, legal, or other non-marketing communications.

9. California Disclosures

This section supplements this Privacy Policy for California residents and serves as our notice at collection where applicable.

During the preceding 12 months, we may have collected the categories of personal information identified in Section 2, from the sources and for the purposes described in Sections 2 and 4. We may disclose those categories to the recipients described in Section 5.

California residents may exercise the rights described in Section 8, including the right to know, delete, correct, opt out of sale or sharing, limit certain uses of sensitive personal information, and receive equal service and price. California residents may also designate an authorized agent, subject to verification requirements.

California residents may request information about certain disclosures of personal information to third parties for their direct-marketing purposes under California Civil Code section 1798.83 by emailing **dataprivacy@ncco.com** with the subject line **"California Shine the Light Request."**

10. State-Specific Information

Residents of certain U.S. states may have the rights described in Section 8, subject to applicable legal exceptions and NCCO's obligations under the relevant law. These rights may include access, correction, deletion, portability, and opt-outs from sale, targeted advertising, and certain profiling.

This Privacy Policy is intended to provide disclosures required by applicable state privacy laws, including, where applicable, the Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Indiana Consumer Data Protection Act, Iowa Consumer Data Protection

Act, Kentucky Consumer Data Protection Act, Maryland Online Data Privacy Act, Minnesota Consumer Data Privacy Act, Montana Consumer Data Privacy Act, Nebraska Data Privacy Act, New Hampshire Privacy Act, New Jersey Data Privacy Act, Oregon Consumer Privacy Act, Rhode Island Data Transparency and Privacy Protection Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act.

Nothing in this section limits rights that apply to you under law. Rights, obligations, and applicability vary by jurisdiction and may depend on statutory thresholds and exemptions. You may exercise your state privacy rights by contacting as set forth below.

11. Data Security

We maintain reasonable and appropriate administrative, technical, and physical safeguards designed to protect personal information against accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use. No method of transmission over the internet or method of electronic storage is completely secure; therefore, we cannot guarantee absolute security.

If you have an account, you are responsible for maintaining the confidentiality of your credentials and for promptly notifying us of suspected unauthorized access to your account.

12. Children's Privacy

The Services are not directed to children under 13 years of age, and we do not knowingly collect personal information from children under 13 without verifiable parental consent. If you believe that a child under 13 has provided personal information to us, contact us at **dataprivacy@ncco.com** so that we can investigate and take appropriate action.

If NCCO operates a Service directed to children or has actual knowledge that it collects personal information from children, we will provide the applicable notice and obtain any required verifiable parental consent before collecting, using, or disclosing that information.

13. International Users

The Services are operated from the United States. Personal information may be processed and stored in the United States and in other locations where we or our service providers operate. Those locations may have privacy laws that differ from the laws of your jurisdiction.

Additional information about international processing of personal information can be found at the following link: https://www.ncco.com/wp-content/uploads/2026/10/NCCO-Privacy-Policy-Supplemental.pdf

14. Third-Party Links and Services

The Services may link to third-party websites, applications, content, or services. We are not responsible for the privacy practices of those third parties. We encourage you to review the privacy notice of each third party before providing personal information or using its services.

15. Student Data

This section of this Policy governs the receipt, access, use, safeguarding, and return or destruction of Student Data that we receive from educational institutions (the "Institution") for the limited purpose of providing educational services to students and related testing and certifications (the "Services"). This Provision is intended to support compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. Part 99, and related state laws. Notwithstanding any other provision, Student Data will be treated as follows.

Definitions

- "Student Data" means any data or information that is directly related to a student and is maintained by the Institution and provided to us on behalf of the Institution, including education records and personally identifiable information as those terms are used in FERPA and 34 C.F.R. Part 99, and in particular Student Data can includes student name, email, phone, usernames, passwords, student identification numbers, IP addresses, test scores, test observation data, test attempts, pass/fail status, certificates, audit logs, proctoring artifacts, language spoken, information about special accommodations, and survey/questionnaire responses.

- "Disclose" and "Disclosure" mean any release of, transfer of, provision of access to, or other communication of Student Data to any person or entity by any means.

- "Authorized Users" means our personnel who have been granted access to Student Data based on a legitimate need to access Student Data to perform the Services, and (b) are subject to confidentiality obligations consistent with this section of the Policy.

- "Security Incident" means any actual or reasonably suspected unauthorized access to, acquisition of, use of, or Disclosure of Student Data, or any event that materially compromises the confidentiality or integrity of Student Data.

We only access, use, and maintain Student Data solely to perform the Services for the Institution and for no other purpose. We do not sell, rent, or license Student Data. We do not use Student Data for targeted advertising/marketing to student accounts. We do not provided Student Data to third parties for marketing purposes. We do not use Student Data in association with any tracking. We do not anonymize or de-identify Student Data.

We do not Disclose Student Data to any third party except (a) as expressly authorized in writing by the Institution, (b) to subprocessors necessary for use to perform the Services as approved by the Institution, (c) to third parties that provide audits certifications that are a part of the Services, and (d) as required by applicable federal law, in which case the we shall, to the extent permitted by law, provide the Institution prompt written notice sufficient to allow the Institution to seek protective relief.

We shall request, access, use, and maintain only the minimum amount of Student Data reasonably necessary to perform the Services, and shall configure workflows to avoid collection or retention of Student Data not required for the Services.

We will implement and maintain reasonable administrative, technical, and physical safeguards designed to protect the confidentiality and integrity of Student Data and to prevent unauthorized access, use, or Disclosure consistent with our written obligations to the Institution that provided the Student Data including those relating to Security Incidents.

The retention of Student Data is determined by the Institution, subject to certain exceptions as approved to the Institution as necessary to meet audit, regulatory, and certification standards associated with the Services provided.

You should understand that we are merely a custodian of Student Data on behalf of the Institution which controls the Student Data. You should consult with the Institution with regard to exercising any of your rights under law regarding Student Data. You can contact us with questions regarding Student Data as set forth below.

16. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. We will post the updated version on this page and revise the "Last Updated" date above. If we make material changes, we will provide additional notice where required by law, such as through the Services, by email, or by another appropriate method.

17. Contact Us

For questions, comments, or requests concerning this Privacy Policy or our privacy practices, contact us at:

National Checking Company
899 Montreal Circle
St. Paul, MN 55102
Email: **dataprivacy@ncco.com**