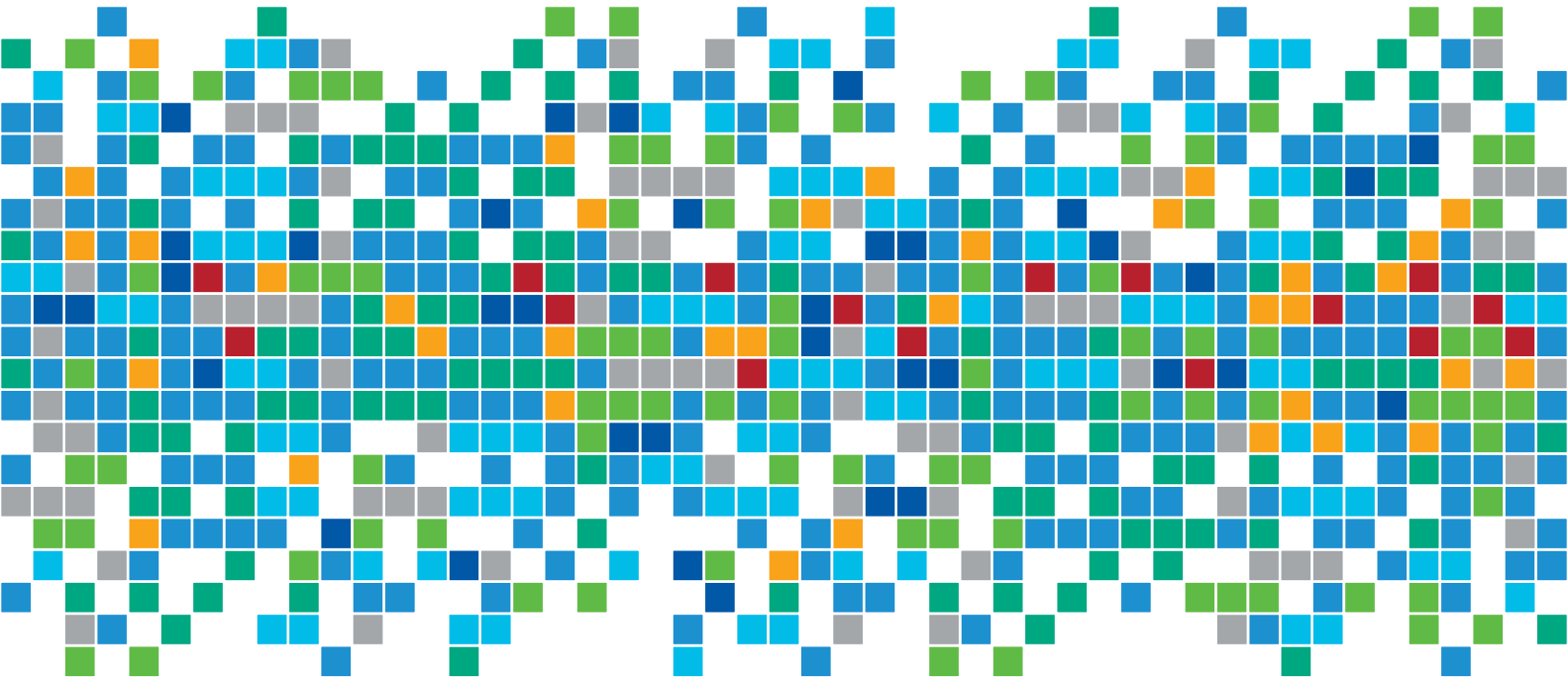




CFA Institute

VOLUNTEER AND NON-EMPLOYEE HANDBOOK



April 2023

Table of Contents

VOLUNTEER AND NON-EMPLOYEE HANDBOOK

- Acknowledgment..... 1
- Policies and Practices for Volunteers and Non-Employees 2
- Information Protection Policy Summary 3
- Customer Credit Card Security Policy 4
- Workplace Safety and Inspections 6
- Dress Code 7
- Equal Opportunity..... 8
- Workplace Accommodations 9
- Travel..... 10

VOLUNTEER AND NON-EMPLOYEE HANDBOOK

Acknowledgment

I, the undersigned, acknowledge receipt of the CFA Institute Handbook For Volunteer and Non-Employee Personnel (the “Handbook”), which sets forth the workplace policies applicable to temporary workers, independent contractors, consultants and volunteers who perform services for CFA Institute (“Non-Employee Personnel”). I also acknowledge my obligation to read, understand, and comply with the Handbook’s contents.

Additionally, I acknowledge that I have read, understand, and comply with CFA Institute’s Code of

Conduct, the Benchmark, which has been provided to me, along with this handbook. If I have questions regarding the contents of either the handbook or the Benchmark, I will consult with my CFA Institute liaison.

SIGNATURE

DATE

FULL NAME (typed or printed)

Policies and Practices for Volunteers and Non-Employees

The Benchmark - Code of Conduct

In addition to the policies in this Handbook, all non-employee personnel performing services for CFA Institute must be familiar with and abide by [The Benchmark](#). Violations of the policies in this handbook or the Benchmark may result in disciplinary action, which may include termination of services performed with CFA Institute. Any questions about sections of The Benchmark should be directed to your CFA Institute liaison or your People Leader.

Information Protection Policy Summary

The Information Protection Policy (IPP) (see business liaison for policy) is a compilation of the policies created to regulate the handling, confidentiality, and availability of CFA Institute information technology resources and data. This is a summary only. Non-Employee Personnel are responsible for reviewing and complying with the full IPP.

The IPP addresses the proper handling of Highly Confidential Information (HCI). HCI includes, but is not limited to:

- **Personally Identifiable Information** such as name, email, address, date of birth, government identification numbers, employment information and professional complaints or investigations;
- **Bank Account, Payment Card, or other Financial Information;**
- **Health Information** such as in the context of employee Health Insurance Benefits or in the case of employee or candidate disability accommodation requests; and
- **Corporate Intellectual Property** such as our proprietary credentialing assets (exam content, forms/answer books, minimum passing scores, exam results, etc.).

CFA Institute Personnel are personally responsible for safeguarding and monitoring proprietary HCI against unauthorized disclosure, modifications, or destruction.

- HCI must be encrypted when digitally transported, transmitted, or stored.
- Making copies of data should be avoided.
- HCI is intended for distribution within CFA Institute and is restricted to (1) employees; and (2) vendors or consultants who have signed a Legal approved contract with CFA Institute. Contact Legal for assistance.

- CFA Institute Personnel must not email HCI outside CFA Institute unless the data is encrypted by a method approved by the ISO. Contact the IT Help Desk for assistance.
- HCI should not be stored locally, printed, or manipulated by 'cut-and-paste' during a remote session.
- Vendors engaged to collect, process, or store HCI must be reviewed and approved by the Chief Information Security Officer (or delegate) and by the Global Data Privacy Officer (or delegate).

If you know, or have reason to believe, that there has been a breach of security or loss or theft of HCI, report such breach immediately as set forth in the Incident Response Policy.

Customer Credit Card Security Policy

I. Purpose

To protect the credit card information that CFA Institute collects from customers and to comply with Payment Card Industry Data Security Standards (PCI DSS) and the [CFA Institute Privacy Policy](#).

II. Policy

It is the responsibility of every employee, temporary employee, consultant and contractor with building or network access to protect and maintain the security of customer credit card data. Generally, customer cardholder data cannot be transmitted or stored electronically in a readable format, and the data cannot be accessed unless there is a legitimate business need to do so. Access to customer credit card information is limited as appropriate to each individual who has a need to view the information to perform their duties. The following are key points:

- Customer credit card information (full account number, last four digits of account number, expiration date, etc.) cannot be entered, forwarded, or stored in:
 - » spreadsheets, documents or Access databases
 - » Siebel service requests, service request notes, or activities
 - » emails or any other electronic files
- The payment card security code (the three-digit or four-digit validation number printed on the front or back of a customer's payment card) cannot be requested or stored in any format.
- Specifically, designated paper forms may be utilized by the Charlottesville Global Contact Center and the Member Affiliation Team only to collect single credit card transactions and are the only paper documents approved for the collection of credit card information via telephone.

- Registrations & Revenue and the Charlottesville Global Contact Center are the only departments authorized to process credit card charges. All paper, fax, and mail credit card transactions must be processed by the Registrations and Revenue (R&R) department only.
- If paper documents containing customer credit card information are received by individuals in other departments or offices, they must be handled as follows:

Charlottesville, VA USA

- » Hand-deliver to R&R staff person or place in R&R's secure incoming mail cabinets.

All offices other than Charlottesville

- » Fax to R&R's secure fax line at (434) 951-5240. Originals must be securely destroyed once receipt is confirmed.

Interoffice mail is not to be used.

- Internal and external forms requesting payment information must have remittance instructions to the R&R post office box number (2082) and/or to the R&R secure fax number (434-951-5240).
- Contracts with third party service providers that collect customer Cardholder Data must be reviewed by the Information Security Officer (ISO), Treasurer and Legal prior to execution.
- Exceptions to this policy must be pre-approved by the ISO in writing.

If you have any questions about these requirements, please contact the ISO or Manager, Registration and Revenue.

III. Responsibilities

All employees are required to acknowledge receipt and understanding of this policy at the start of their employment and at least annually thereafter. All temporary employees, consultants and contractors with building or network access are required to

Customer Credit Card Security Policy (continued)

acknowledge receipt and understanding of the Information Protection Policy (which includes the security of cardholder data) at the start of their contractual relationship and at least annually thereafter.

This policy is applicable to CFA Institute, its affiliates, and its subsidiaries.

Workplace Safety and Inspections

All individuals on company property are expected to obey posted safety rules and to exercise caution in all work activities. Individuals must promptly report any unsafe condition to the appropriate people leader.

CFA Institute is committed to maintaining a safe work environment for all employees, non-employees, and visitors. In doing so, CFA Institute reserves the right to take appropriate measures toward this goal that may include the use of such devices as video surveillance equipment, both visible and concealed, on company premises.

CFA Institute may monitor the general areas of the facility including but not limited to all interior office space, common areas, and parking lots. Employees, workers, and guests should not have any expectation of privacy in these areas.

To the extent permissible under applicable laws, CFA Institute prohibits the possession, transfer, sale, or use of illegal drugs, alcohol, firearms, explosives, or other improper materials on its premises and requires the cooperation of all in administering this policy.

For everyone's safety, if CFA Institute reasonably suspects that an individual possesses items that are prohibited on CFA Institute premises, the property may be searched, in accordance with applicable laws. This may include personal property such as a cooler, purse, briefcase, vehicle, etc., and assigned company property such as offices, desks, drawers, lockers, workspace, computer files, etc. Please remember that individuals on CFA Institute property should not have any expectation of privacy in any item that is company property, even if they have company assigned items such as a desk or locker or access codes.

Dress Code

The CFA Institute Dress Code Policy outlines the parameters for presenting oneself in a professional manner, and is not intended to be a complete set of rules or an all-inclusive list of items that are allowed or not allowed. Rather, Non-Employee Personnel are expected to use the policy as a guide and exercise good judgment when selecting work clothing.

All clothing should be clean and in good repair (without holes and tears — even if purchased this way) and must support our goal of creating a welcoming and safe environment that embraces differences, demonstrates respect, and instills trust. Regardless of the circumstances, shorts are not considered an appropriate clothing choice. Non-Employee Personnel are encouraged to speak with their CFA Institute liaison if they have questions about making appropriate clothing choices consistent with this policy.

There may be medical conditions and/or particular CFA Institute positions that require exceptions to this policy all or some of the time. CFA Institute will also make reasonable accommodations to its Dress Code for a Non-Employee Personnel's bona fide religious beliefs or practices. Please speak with your CFA Institute liaison if you have any questions.

Equal Opportunity

It is the established policy of CFA Institute not to discriminate against any individual employee or Non-Employee on the basis of race, any traits historically associated with race, color, national origin, citizenship or immigration status, religion, creed or belief, age, marital or partnership status, marital or family status, care giver status, pregnancy and maternity, breastfeeding, sexual and other reproductive health decisions, physical abilities/qualities, disability, sexual orientation, gender, gender identity or expression, predisposing genetic characteristic, military or veteran status, status as a victim or witness of domestic violence or sex offense or stalking, unemployment status, infectious disease carrier status, migrant worker status, educational background, socio-economic status, geographic location and culture or any other basis protected by applicable law. This policy impacts all aspects of employment, including but not limited to, recruitment, training, development, promotion, demotion, and dismissal. This is a global policy that applies to all CFA Institute employees and Non-Employee Personnel, regardless of location.

Any Non-Employee Personnel who feels that they have experienced or witnessed discrimination under this policy should promptly notify their primary employer or temporary staffing agency, if applicable, and then their CFA Institute liaison.

Non-Employee Personnel may raise good faith concerns and make reports without fear of reprisal. Any Non-Employee Personnel found to be engaging in any type of discrimination or retaliation in violation of this policy will be subject to termination of services for CFA Institute.

Workplace Accommodations

I. Workplace Disability or Pregnancy Accommodations

Non-Employee Personnel who are pregnant or who are qualified individuals with disabilities covered by applicable disability laws, and who require reasonable accommodations should first discuss potential accommodations with their primary employer or temporary staffing agency, if applicable, and then with their CFA Institute liaison.

II. Workplace Religious Accommodations

Non-Employee Personnel whose religious beliefs or practices conflict with their duties, work schedule, CFA Institute Dress Code, or with other aspects of services for CFA Institute, and who seek a religious accommodation should first discuss their request with their primary employer or temporary staffing agency, if applicable, and then with their CFA Institute liaison.

Travel

All Non-Employee Personnel who engage in travel for CFA Institute business are responsible for reading and abiding by the terms of the CFA Institute Non-Staff Travel Policy, which is available on the CFA Institute [website](#). The objective in developing the policy is to provide for the well-being of non-staff while traveling on behalf of CFA Institute, and ensuring the best value is obtained using available savings programs and reasonable cost management.

Questions should be directed to your CFA Institute liaison.