



Policy No: HR114
Created: May 2026
Updated:

Confidentiality Policy

Cutting Edge Renovation & Painting expects employees to protect confidential, sensitive, and nonpublic information learned or accessed during employment. Employees may have access to Company information, customer information, job details, pricing, estimates, employee information, vendor information, financial information, internal procedures, and other information that should not be shared outside the Company.

Employees are expected to use confidential information only for legitimate Company business and to protect it from unauthorized use, disclosure, loss, or misuse.

Purpose

The purpose of this policy is to help protect the Company, customers, employees, vendors, and business operations by explaining how confidential information should be handled.

This policy applies to all employees and to all forms of confidential information, whether spoken, written, printed, electronic, photographed, saved in Company systems, sent by text or email, or learned during work.

Confidential Information

Confidential information may include, but is not limited to:

- Customer names, addresses, phone numbers, emails, and job details
- Customer photos, videos, home information, or property details
- Estimates, bids, proposals, pricing, and discounts
- Vendor pricing, supplier terms, and purchasing information
- Employee records, payroll information, disciplinary records, or personal information
- Company financial information
- Business plans, marketing plans, sales information, and internal reports
- Company forms, processes, procedures, checklists, and training materials
- Passwords, login information, software access, and system information
- Jobsite concerns, complaints, investigations, or legal matters
- Any nonpublic information related to Company operations

Employee Responsibilities

Employees are responsible for protecting confidential information and using it only as needed to perform their job duties.

Employees must:

- Keep confidential information secure
- Share confidential information only with employees or authorized individuals who have a business need to know
- Avoid discussing confidential matters in public areas or around customers, vendors, or others who do not need the information
- Protect printed documents, electronic files, photos, messages, and records
- Avoid leaving confidential documents or devices unattended
- Report lost, stolen, or improperly shared information to HR or management right away

Customer Information

Employees may not use or share customer information for personal purposes, side work, outside employment, or non-Company business.

Customer information includes, but is not limited to:

- Names
- Addresses
- Phone numbers
- Email addresses
- Jobsite access information
- Photos or videos of the home or business
- Project details
- Pricing, estimates, or invoices
- Personal information learned while working at the customer's home or business

Employees may not contact Company customers for personal work or share customer information with anyone outside the Company unless approved by management.

Additional expectations related to side work and customer relationships are covered in **Policy HR113: Conflict of Interest and Outside Employment Policy**.

Photos, Videos, and Social Media

Employees may not post or share customer homes, businesses, jobsite photos, videos, coworkers, Company work, behind-the-scenes content, or customer information on personal social media without approval from management.

This includes photos or videos shared through:

- Facebook
 - Instagram
 - TikTok
 - Snapchat
 - Youtube
- 

- Personal websites
- Text messages
- Group chats
- Online forums
- Any other public or private platform

Only authorized Company representatives may post Company-related content for marketing, advertising, or public communication purposes.

Employee Information

Employee records and employee-related information must be kept confidential. Employees may not share another employee's personal, payroll, medical, disciplinary, attendance, performance, or employment information unless authorized and needed for legitimate Company business.

This policy does not prohibit employees from discussing their own wages, hours, or other terms and conditions of employment as allowed by law.

Company Documents and Records

Company documents, forms, templates, checklists, estimates, pricing sheets, training materials, customer lists, job records, and internal procedures are Company property.

Employees may not copy, remove, save, forward, photograph, distribute, or use Company records for personal purposes, side work, outside employment, or competing business activity without authorization.

Electronic Information and Passwords

Employees must protect Company electronic information, including files, apps, email, text messages, photos, videos, job notes, software, and system access.

Employees may not:

- Share passwords or login information unless authorized
- Access company systems without a business reason
- Download, copy, or forward company information without authorization
- Use personal accounts to store company information unless approved
- Delete or alter company records without authorization
- Allow unauthorized individuals to access Company systems or devices

Additional expectations related to phones, apps, electronic communication, and Company systems are covered in **Policy HR111: Technology, Phone, and Communication Policy**.

Investigations and Internal Matters

Employees are expected to keep workplace investigations, disciplinary matters, complaints, employee concerns, legal matters, and sensitive business issues private.



Information about these matters should only be shared with HR, management, or individuals who have a legitimate business need to know.

Protected Employee Rights

Nothing in this policy is intended to limit or interfere with employee rights under applicable law.

This policy does not prohibit employees from:

- Discussing wages, hours, or working conditions
- Reporting safety concerns
- Reporting harassment, discrimination, retaliation, wage concerns, or legal violations
- Participating in a workplace investigation
- Filing a complaint with a government agency
- Cooperating with a government agency investigation
- Engaging in other legally protected activity

Return of Confidential Information

Upon request or at the end of employment, employees must return all Company documents, files, records, devices, keys, tools, materials, and any other Company property.

Employees may not keep copies of confidential Company or customer information after employment ends unless authorized by management or required by law.

Violations

Unauthorized use, disclosure, copying, removal, or misuse of confidential information may result in corrective action, up to and including termination of employment.

Examples of violations include:

- Sharing customer information without approval
- Using customer information for side work
- Posting jobsite photos or customer property without approval
- Sharing pricing, estimates, or internal documents with unauthorized individuals
- Disclosing employee information without authorization
- Using company records for personal business
- Sharing passwords or login access
- Keeping Company documents after separation of employment

Questions

Questions about confidential information, customer privacy, Company records, photos, social media, or proper handling of information should be directed to HR or management.

