

WEBSITE POLICY



02.23.2021 | Responsible Party: Marketing Director

Table of Contents

- Introduction 3
 - Objective 3
 - Statement of Purpose 3
 - Responsibility of Policy 3
 - Compliance and Legal Risks..... 4
 - Web Content Management..... 4
 - Information Collection and Sharing 4
 - SECURITY..... 5
 - Change in Management 5
 - 3rd Party Responsibility 5
 - Google Analytics..... 5
 - Web Linking 6

Introduction



This website policy discloses the privacy and security practices for www.community1st.com and www.hfgtrust.com. This policy applies solely to information on these websites. The combined entities will be referred throughout this document as “The Company”.

Objective

It is the policy of The Company to utilize the websites as an effective information tool to educate clients about our products and services. Our website is a dynamic and evolving technology and any definition listed above is meant to be illustrative and not exhaustive.

Community First Bank and HFG Trust recognize the importance of having an updated online presence, a platform to engage and inform our clients, prospective clients and community.

Statement of Purpose

The Company recognizes there are inherent risks with having a website. Websites poses compliance, reputational, operational, legal risk and even risk of harm to consumers and The Company. Therefore, the Board has approved this Website Policy to facilitate both direction and guidance to mitigate such risk.

The content of the pages of this website is for your general information and use only. It is subject to change without notice. This website contains material which is owned by or licensed to The Company. This material includes, but is not limited to, the design, layout, look, appearance and graphics. Reproduction is prohibited other than in accordance with the copyright notice, which forms part of these terms and conditions.

Responsibility of Policy

The Marketing Director and Director of IT are responsible for ensuring compliance with this policy. The Marketing Director and IT Department will consistently review and recommend changes to this policy as they deem applicable for compliance and risk mitigation. Any violation of this policy must be promptly reported to the responsible parties.

Compliance and Legal Risks

Compliance and legal risk arise from the potential for violations of, or noncompliance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. Failure to adequately address these risks can expose The Company to enforcement actions and/or civil lawsuits. If The Company is to update content on the website to market products, new accounts and promote brand awareness, The Company will take appropriate steps to ensure that advertising, account origination, and document retention are performed in compliance with applicable consumer protection and compliance laws and regulations.

Web Content Management

Content that appears on these websites will ensure that brand consistency is followed and represents The Company in a positive light. All pages and content will be housed within the website's WordPress Content Management System for proper reporting of activity.

Information and media that is published to The Company's websites, including but not limited to product pages, written blogs, video content, white papers, financial reports, and promotions will be reviewed by the Marketing Director prior to publishing. Additionally, web content including information about individual departments of The Company, will be first approved by the departments' stakeholders prior to publishing. Updates and changes to website content are subject to all other guidelines reflected in the policy.

Information Collection and Sharing

We are the sole owners of the information collected on this site. We only have access to information that visitors voluntarily give us via email or other direct contact from a client. Our intention is not to sell or rent information to anyone.

We will use all information provided to respond to clients and prospects, regarding the reason they have contacted us. We will not share their information with any third party outside of our organization, other than as necessary to fulfill your request, e.g. to ship an order.

Unless the client or prospect specifically asks us not to, we may contact them via email in the future to tell them about promotions, new products and services and changes to company policies.

SECURITY

We take precautions to protect client and company information. When sensitive information is submitted via the website, the information is protected both online and offline. You can verify this by looking for a closed lock icon at the bottom of your web browser, or looking for "https" at the beginning of the address of the web page. While we use encryption to protect sensitive information transmitted online, we also protect client's information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment and will not be present on our website.

Change in Management

Our website works with a list of external management systems. If there is a change in system management, our procedural manual will outline the necessary steps to remove the existing vendor and approve a replacement.

3rd Party Responsibility

Regularly updating and maintaining our website is crucial to ensuring that our site operates at full capacity. The Company website utilizes Word Press Content Management System and will routinely look for patch updates. Failing to do so will leave our website susceptible to hacking and data breaching. As more end user systems can leave the network, patching frequency becomes more important. For example: Microsoft may keep to a predictable security patch release cycle (Patch Tuesday, second Tuesday of every month, except February 2017), but most other vendors have unpredictable release schedules. We have outsourced this responsibility to a third party to ensure word press patches are updated frequently. They provide a monthly report and analysis identifying possible threats and activity on our website.

Google Analytics

We use a tool called "Google Analytics" to collect information about use of The Company site. Google Analytics collects information such as how often users visit this site, what pages they visit when they do so, and what other sites they used prior to coming to this site. We use the information we get from Google Analytics only to improve this site. Google Analytics collects only the IP address assigned to visitor on the date they visit our site, rather than personal information. We do not combine the information collected

through the use of Google Analytics with personally identifiable information. Although Google Analytics plants a permanent cookie on a visitor's web browser to identify them as a unique user the next time they visit our site, the cookie cannot be used by anyone but Google. Google's ability to use and share information collected by Google Analytics about visitors information is restricted by the Google Analytics Terms of Use (as amended for government websites) and the Google Privacy Policy. All visitors can prevent Google Analytics from recognizing them on return visits to this site by disabling cookies on their browser.

Web Linking

A web linking relationship is a third party vendor that is linked directly to our website. Any website managed by the company will utilize an external link warning notifying users that they are leaving the bank's website. Approving third party links involve a review by the resident department manager (i.e. Lead Mortgage Officer, Chief Lending Officer) and the Market Director for credibility and security. Our procedural manual will outline how a third party becomes eligible and the process of creating new web linking relationships.