Technology & Internet Usage Policy

Title Block	
Document Name: TECHNOLOGY & INTERNET USAGE POLICY	##
Committee Approval Date:	**Dept./Individual Responsible for Maintaining/Updating:**
Board Approval Date: **6/15/22**	**Review Cycle Schedule:** Annually

Table of Contents

Technology & Internet Usage Policy

I. INTRODUCTION

Technology is a tool that can benefit every department within our bank. Through its efficiencies, it improves customer service, retention, growth and productivity. Therefore, it is the policy of bankcda that employees will be provided with the appropriate technology to do their jobs. When we speak of technology, we are including our telephones computers and peripheral equipment such as printers and scanners, e-mail access, Internet access and usage, and mobile devices.

Additionally, the bank encourages the use of social media to help to build stronger, more successful business relationships. The bank has an overriding interest and expectation in deciding what is "spoken" on behalf of the bank on social media sites, and therefore has established guidelines for employee participation for both off-duty and official participation.

Access to the Internet, e-mail and any specific computer equipment will be approved on an as-needed basis. Management will also determine any limitations to this usage. All employees utilizing the technology provided by the bank, either hardware, software or on a bank-owned domain name or on a bank Internet access account—whether doing business for the bank or for personal uses—should agree to the conditions and requirements of this policy.

As a good corporate citizen, the bank has a responsibility to help make all the technology offered safe, secure, and productive business tool for our employees, customers, and non-customers.

II. POLICY OVERVIEW

This Technology Usage Policy is designed to help our employees understand the bank's requirements and expectations for the use of the technology available. This policy distinguishes between usage during the employee's working hours and that performed on personal time (i.e., weekends, before and after work, lunch periods, or breaks). Personal use is allowed provided it in no way interferes with the intended business uses of the bank's resources, Internet, and technology equipment nor incurs unnecessary costs to the bank without prior authorization. All personal use must also be in accordance with the restrictions and requirements established in this policy.

Unnecessary or unauthorized usage causes congestion, particularly excessive use of the Internet. It slows other users' access, reduces effective work time, consumes supplies, and ties up printers and other shared resources. For the most part, personal usage of the bank's technology should be kept to a minimum during work hours.

You are required to conduct yourself appropriately while using all forms of bank technology. Proper use requires that you respect all copyrights, software licensing rules, property rights, and the privacy of others, just as you would in your day-to-day business activities. You are cautioned not to use our technology for any purpose that would reflect negatively on the bank, its employees, or subsidiaries.

Do not make any comment that may be misrepresented as being the bank's position unless you are

empowered to make such a comment. Unlawful Internet/social media usage in particular may contribute to reputation risks and expose the bank to legal liabilities.

It is important for you to understand that how you communicate through social networking sites, even when you are off-duty, could impact the banks reputation. Whether or not you decide to participate in an online forum, networking site or blog on your own personal time is your decision. However, the way the bank is represented on these online sites is of utmost importance. Since information posted on the Internet is available to the public, the bank has established the following guidelines for your participation in social media.

All bank e-mail and/or Internet users must agree to the following statement and positively affirm the statement with a signature. The statement will be filed with your personnel records.

"I fully understand the terms of this policy and agree to abide by them. I realize that the bank may incorporate monitoring software and may record, for management use the Internet address of any site I visit. The bank may keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive can be recorded and stored in an archive file for management's use. These archives may be accessed by law enforcement agencies when required legal processes are executed. I know that any violation of this policy could lead to dismissal or applicable criminal prosecution."

The Internet is a business tool. Access is for business-related purposes, i.e., to research relevant topics; communicate with customers, vendors, and regulators; and obtain useful business information [except as outlined below in III. 17].

III. POLICY PROVISIONS

1. The bank may have in place and use, at any time, the software and systems to monitor and record all e-mail and Internet activities. These systems are capable of recording (by user) each World Wide Web site visited, chat, newsgroup, or e-mail message and each file transferred into and out of our internal networks. We reserve the right to do so at any time. No user should have any expectation of privacy as to e-mail or Internet usage. Assigned individuals may review Internet activity logs and report suspicious findings to the appropriate supervisor or member of management.

2. The bank reserves the right to inspect any and all files stored on bank-owned hardware and on any personal media brought on bank premises by employees to ensure compliance with this policy.

3. The purposeful display or verbal transmission of any kind of sexually explicit or discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability) image or document on any

bank computer, fax machine, voicemail or other device is a violation of this policy. In addition, none of these files may be archived, stored, distributed, edited, or recorded using bank resources.

4. The bank may use approved software to identify inappropriate or sexually explicit Internet sites. These sites may be blocked from access based on some specific or general criteria. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any filtering program, and report it to your supervisor.

5. Inappropriate uses of the bank's equipment, voicemail, hardware, software, and Internet connectivity include:

a. Uploading, downloading, recording or otherwise knowingly accessing or transmitting in any fashion:

i) Abusive, hateful, degrading, demeaning, derogatory or defamatory materials, information, or communications. Emphasis is added as it pertains to race, color, religion, national origin, gender, sexual orientation, political beliefs, or disability.

ii) Pornographic, obscene, sexually explicit, indecent, or vulgar materials, information, or communications.

iii) Any confidential records of the bank, its customers, or vendors without adequate authority to do so. Employees must know what is and is not acceptable based on their position and function within the bank.

iv) Any materials or programs, including access and registration codes, which are in violation of copyright protections.

v) Any trade secrets, rude or abusive language, or negative characterizations of others or of the bank.

vi) Resumes or other activities related to seeking employment outside of our organization unless expressly authorized to do so.

vii) Chain letters, distasteful jokes, gambling of any nature.

viii) Solicitations or advertisements for other than the bank, its affiliates, or subsidiaries unless authorized.

ix) Any virus, worm, Trojan horse, or trap door program code.

x) Any attempt to disable or overload any computer system or to circumvent any system intended to protect the privacy or security of another user.

b. Vandalizing, damaging, disabling, or gaining access to another entity's computer files or data. 18 U.S.C. §1030 prohibits unauthorized individuals from accessing a computer or its data and from damaging either. This can result in a fine or imprisonment.

c. Sending e-mail, voicemail, or otherwise transmitting anything anonymously or under an alias unless authorized.

d. Engaging in any other activity restricted by local, state, federal, or international laws. Use of any bank resources for illegal activity will be grounds for immediate dismissal. The bank will cooperate with any legitimate law enforcement activity.

6. Any files downloaded via the Internet or transmitted onto a bank computer or other device becomes the property of the bank. Any such files may be used only in ways that are consistent with applicable licenses or copyrights.

7. Personal views cannot be presented as though they are that of the bank. Unless authorized to do so in the performance of your duties, employees may not speak or write in the name of the bank. Employees must refrain from any unauthorized endorsement or appearance of endorsement by the bank of any commercial product or service not sold or serviced by the bank, its subsidiaries, or its affiliates.

8. Subscribed services, whether free or on a cost basis (i.e., newsgroups, listservs, etc.), and participation in chat sessions will require prior bank approval.

9. When participating in any newsgroup or chat session or when sending e-mail, voicemail or fax, it is inappropriate to reveal confidential information, customer data, or trade secrets without proper customer verification.

10. All outgoing e-mail and postings to internal employees, newsgroups, listservs, etc., must be reviewed just as though it were traditional correspondence. Improper spelling and grammar reflect poorly on the professional image of the bank and its employees.

11. No software should be downloaded or installed without prior authorization from IS and appropriate department management.

12. Use of the Internet for extended periods of time, such as file downloads longer than 15 minutes each, video and audio streaming. Internet Channels or other recurring, regularly scheduled downloads, will be permitted on a case-by-case basis. These activities should be completed during non-peak periods if at all possible.

13. Any employee who attempts to disable or circumvent any bank security program or device will be in violation of this policy and subject to personnel actions.

14. Although customer service is vital to our success, so is our obligation to help prevent identity fraud against any of our customers. For this reason, employees will not reveal confidential

customer information in response to an e-mail or voice-mail request unless the identity of the customer (mail sender) is **absolutely verified**. Files containing sensitive bank or customer data that are transmitted in any way over the Internet must be encrypted or password-protected in a bank-approved manner. The decryption key or password should be transmitted to the intended receiver by another means, such as conventional mail or telephone. Exceptions must be approved by the a member of Senior Managementand should be rare.

15. User identifications and passwords help maintain individual accountability for technology usage. These are meant to be confidential. Bank policy prohibits the sharing of user identifications or passwords for use of any bank computer or other device ***(see end user computing policy for detailed password policy).***

16. Technology at work is for bank use. However, when certain criteria are met, employees are permitted to engage in the following activities:

a. During work hours, employees may access the internet for job-related information to perform specific job requirements.

b. During work hours, employees may participate in newsgroups, chat sessions, e-mail discussion groups (listservs), and social media posting, provided these are job performance-related. If personal opinions are expressed, a disclaimer should be included clearly indicating that this is not an official bank position.

c. During non-work hours, employees may retrieve non job-related text and graphics to develop or enhance Internet-related skills. This access is allowed to enhance the employee's skill set and should improve the accomplishment of job-related work assignments. Adherence with this policy, and in particular, Sections III. 5 – 12, is required. If the employee's Internet connection is shared, either on a shared computer or peripheral, business conducted by an employee conducting official business will take precedence when there is a time-use conflict.

d. Employees are prohibited from initiating non work-related Internet access using bank resources from remote locations.

17. As a rule, "the bank" will not use social media applications to expressly sell our products; they will be primarily used for:
    - Engaging with, informing and responding to customers (with the exception of confidential information)
    - Publicizing sponsored events, seminars, etc.
    - Sharing photos and videos of sponsored events, seminars, offices, etc.
    - Soliciting customer and/or community feedback
    - Monitoring information about the bank
    - Keeping our brand fresh and up-to-date

    .
18. Social Media Documentation files will be used as a way to manage social media accounts and track complaints as well as keep a record of all account activity for retention purposes. Records

of activity will be retained and accessible for as long as the history is available on the system. Complaints will be flagged as complaints and responses to complaints will be accessible via Social Media Documentation files

IV. TRAINING

All employees using the technology provided by the bank will receive the appropriate training on an ongoing basis. All who participate in social media on behalf of the bank for work-related purposes are expected to be trained, to understand and to follow these guidelines. It is the responsibility of the eBanking Coordinator to manage all social media accounts including updating or commenting on the bank's social media accounts and may designate authorization to additional employees for assistance. The eBanking Coordinator is also responsible for monitoring the account on a frequent basis to record communications and to address any posts that are in need of feedback.

V. AUDIT

Internal audits will be completed periodically. The scope of the audit will include a review of users' pc to determine that no unauthorized software has been loaded. A review of the "C" drive will also be completed to what Internet sites have been visited by that employee. Violations will be reported to the employee's supervisor and/or senior management, depending on the severity and frequency of the violations.

VI. RECORD RETENTION

All incoming correspondence (e-mail) will be retained for not less than 30 days and no longer than 60 days. If it involves a dispute of any kind under investigation, retention will be indefinite.

Social Media Documentation files will be used as a way to manage social media accounts and track comments as well as keep a record of all account activity for retention purposes. Records of activity will be retained and accessible for as long as the history is available on the system. Complaints will be flagged as complaints and responses to complaints will be accessible via Social Media Documentation files.

Correspondence particular to the availability of credit, an inquiry on an existing mortgage loan, any claim of unauthorized use of a debit, ATM or credit card or reports of lost debit, ATM or credit card will be immediately routed to the designated individual/department [as noted in the bank's applicable Regulation E, Z Policy]. These messages require timed responses and special attention.

Employee discretion should be used with respect to printing messages for retention with other documents for convenience.

VII. POLICY ENFORCEMENT

Violations of this policy may result in disciplinary actions. Depending on the severity or frequency of the violations, the following actions could include:

- Counseling statements for policy violations.
- A suspension/termination of technology use privileges. This could then result in a position/function reassignment, and the employee's compensation package may be affected.
- Termination of employment.
- Personal liability under applicable local, state, federal, or international law#v#
#

In regard to social media we strongly encourage user participation, these are the guidelines we will follow to keep the dialogue safe for everyone:

- We will delete content that is spam, malicious, ugly, offensive, denigrating and completely out of context to a conversation.
- We will keep content that is positive or negative and relevant to the conversation, regardless of whether it's favorable or unfavorable to the bank.
- The bank will respond to all posts in a timely manner, unless a response seems unnecessary or inappropriate.

Acceptable Use Policy, Technology & Internet

Statement of Understanding

I fully understand the terms of this policy and agree to abide by them.

I realize that the bank may incorporate monitoring software and may record, for management use the Internet address of any site I visit.

The bank may keep a record of any network activity in which I transmit or receive any kind of file.

I acknowledge that any message I send or receive will be recorded and stored in an archive file. These archives may be accessed by law enforcement agencies when required legal processes are executed.

I know that any violation of this policy could lead to dismissal or applicable criminal prosecution.

_____ _____

Date Signed

_____

Name