Technology Use Policy

Central Kansas Community Foundation & All Affiliate Foundations

Applicable to staff, board members, volunteers, review committee members, fund advisors, vendors and contractors.

I. Purpose

This policy outlines the acceptable use of technology resources provided by Central Kansas Community Foundation, including hardware, software, and cloud – based services. It is designed to protect the integrity, security, and confidentiality of organizational data which includes personal identifying information, and ensure responsible use by staff, volunteers, board members, fund advisors and contractors. We will also address the use of AI – Artificial Intelligence.

II. Scope

This policy applies to all individuals who access Central Kansas Community Foundation's technology resources, including: – Employees (full – time and part – time) – Board Members – Volunteers – Review Committee Members - Fund Advisors – Contractors, vendors and consultants (as applicable).

III. Technology Resources Covered

Organization – issued laptops and mobile devices
Microsoft 365 Licensed Users (including Outlook, Teams, SharePoint, OneDrive)
Boardable (Board management platform)
Foundant Technologies (CSuite for fund management)
Other cloud – based tools used for organizational operations

A. Acceptable Use

Users must: – Use technology resources only for authorized organizational purposes. – Protect login credentials and never share passwords. – Access only the data and systems necessary for their role. – Store sensitive (private, confidential) documents only in approved cloud platforms (e.g., SharePoint, Foundant, Boardable, Community Force, Wufoo). – Log out of systems when not in use and lock devices when unattended (including laptop and phones). Staff may be utilized to assist with loading and saving files with restrictions in cloud-based platforms, i.e. SharePoint, Foundant, Boardable.

B. Prohibited Use

Unless approved by a supervisor, users must not: – Use organizational devices or accounts for personal purposes. – Download unauthorized software or applications. – Share confidential information outside the organization without proper authorization. – Attempt to bypass security controls or access restricted data.

Users must not use organizational devices or accounts for illegal activities.

IV. Confidentiality and Data Privacy

Central Kansas Community Foundation is committed to protecting the confidentiality and privacy of all data entrusted to it, including but not limited to donor information, financial records, stakeholder data, and internal communications.

All users are expected to: Treat all organizational data as confidential unless explicitly stated otherwise. Refrain from discussing sensitive information in public or unsecured environments. Use only approved platforms (e.g., SharePoint, Foundant, Boardable) for storing and sharing confidential data. Report any suspected data breaches or unauthorized access immediately to a senior CKCF representative.

Comply with all applicable data protection laws and internal privacy policies.
Confidential information may include any and all of the following categories:

- Any information, including demographic, health, and financial information (in paper or electronic form, regardless of how it is obtained, stored, utilized, or disclosed).
- Personal information such as social security numbers, banking information, salaries, employment records, student records, disciplinary actions, etc.
- Financial information such as financial and statistical records, academic, or research funding, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary information, including computer programs, source code, proprietary technology, etc.
- Third – party information such as insurance, business contracts, vendor proprietary information, or source code, proprietary technology, etc.

As a condition of and in consideration of your use, access, and/or disclosure of confidential information:

- You will access, use, and disclose confidential information only as authorized and in the conduct of the specific business purpose for which you are being given access for role with CKCF or one of its Affiliates.
- You will take reasonable and appropriate measures to safeguard the privacy and security of any confidential information that you access, use, or disclose in the conduct of the specific business purpose/function in which you are engaged.
- **Printed materials shared at in person meetings, must be returned to the CKCF staff or board or committee chair in attendance prior to the end of the meeting to maintain privacy and confidentiality.**
- You will immediately notify a senior representative of CKCF if you have reason to believe that privacy or security of confidential information has been compromised.

If you are granted access to CKCF or one of its Affiliates electronic systems in order to access information:

- You will safeguard and not disclose your individual user identification and/or password codes to anyone.
- You will not request access to or use any other person's passwords or access codes unless in circumstances of cross training and back up support for systems in which the organization is aware of the sharing for purposes of internal workflow.
- You accept responsibility for all activities undertaken using your passwords, access code, and other authorizations.
- That device should not be connected to Wi-Fi guest systems (i.e. McDonald's, City Hall). When in remote community settings, devices should be connected to Wi-Fi only through assigned systems, generally hotspot on a CKCF issued phone. Staff with Wi-Fi access at home for remote work approval may utilize their home Wi-Fi if protected with password protection.

Failure to uphold confidentiality and data privacy standards may result in disciplinary action, including termination of access, legal consequences, or removal from the organization.

V. Data Privacy Standards

As a community foundation, CKCF, including all Affiliates, is entrusted with sensitive personal and financial information from donors, grantees, volunteers, and community partners. We are committed to upholding the highest standards of data privacy and security in compliance with applicable federal and state laws.

Key Principles:

1. Lawful and Transparent Data Collection
   Personal data is collected only for legitimate organizational purposes and with the knowledge and consent of the individual, where required.

2. Data Minimization and Purpose Limitation
   Only the minimum necessary data is collected and retained, and it is used solely for the purposes for which it was collected.

3. Access Controls and Confidentiality
   Access to personal and sensitive data is restricted to authorized personnel based on role – specific needs. Confidentiality agreements and training are required for all staff, volunteers, review committee members, board members, and contractors with access to such data.

4. Secure Storage and Transmission
   Data is stored in secure, access – controlled systems (e.g., SharePoint, Foundant, CSuite) and transmitted using encrypted channels. Physical and digital safeguards are in place to prevent unauthorized access, loss, or misuse. Private information to be shared with an external provider (i.e. print shop) must be transported via a flash drive, secure provider platform, or encrypted email. Reminder to delete sensitive information from the flash drive once the information has been transmitted. Do not download private information on your personal device.

5. Data Subject Rights
   Individuals may request access to their personal data, corrections, or deletion, in accordance with applicable laws and organizational procedures.

6. Incident Response and Breach Notification
   Any suspected data breach must be reported immediately. The foundation will investigate and, if necessary, notify affected individuals and authorities in accordance with legal requirements.

7. Ongoing Training and Oversight
   Regular training is provided to ensure all users understand their responsibilities regarding data privacy.

VI. Passwords

A. Password Complexity

Passwords for most CKCF programs shall comply with the following requirements:

- A minimum of eight (8) characters in length
- **Contain three (3) of four (4) of the following categories:**
    - Uppercase
    - Lowercase
    - Numeral
    - Non – alpha numeric character

Users should try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation or other phrase. For example, the phrase might be "This may be one way to remember," and the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Foundation employees and users of certain software applications and issued devices, such as laptops and smartphones, will be required to use multifactor authentication (MFA) to access software systems, i.e. Foundant CSuites, Boardable.

B. Protection of Passwords

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e – mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Passwords must not be shared with others unless for distinct situations of which supervisors are aware.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- PCs must not be left unattended without enabling a password – protected screensaver or logging off the device.

VII. File Access and Permissions

To maintain data integrity and confidentiality, access to digital files and documents stored on platforms such as Microsoft SharePoint, OneDrive, Boardable, Community Force and Foundant Technologies (CSuite) will be managed with appropriate permission levels based on user roles and responsibilities. As a user, you have the responsibility to learn and apply the proper use of each platform you have been given access. In additional to CKCF training, each system has user training guides and resources you may need to access.

Access Controls May Include: Read – Only Access: Users can view documents but cannot edit or delete them. – Download Restrictions: Certain files may be restricted from being downloaded to prevent unauthorized distribution or offline storage. Yet if an item is able to be downloaded yet is of confidential in nature, use best judgement in not downloading or printing such materials. Annotation/Commenting Access: Users may be granted permission to leave comments or annotations without altering the original content. Edit Access: Granted only to authorized personnel who require modification capabilities as part of their role. Restricted Sharing: Users are prohibited from sharing files externally unless explicitly authorized. Audit Trails: Access and activity logs may be monitored to ensure compliance with data security policies.

User Responsibilities: Do not attempt to bypass or alter access controls. Report any access issues or unauthorized access immediately. Use only approved platforms for storing and sharing organizational documents.

These controls are in place to protect sensitive information, ensure accountability, and support compliance with data privacy regulations.

VIII. Device Management

- Organization – issued devices remain the property of Central Kansas Community Foundation and its affiliates.
- Users must report lost, stolen, or compromised devices immediately.
  Upon termination of employment or volunteer service, all devices and access credentials must be returned or deactivated.

IX. Use of Artificial Intelligence (AI)

CKCF recognizes the growing role of Artificial Intelligence (AI) tools in enhancing productivity, communication, and decision-making. To ensure responsible and ethical use, the following guidelines apply to all staff, volunteers, and board members when using AI technologies in the context of organizational work:

A. Permitted Use:

AI tools may be used to support tasks such as drafting communications, summarizing documents, analyzing data, and automating routine workflows.

Only approved AI platforms and tools may be used for organizational purposes. Use of third – party AI tools must be reviewed and authorized by the supervisor or CKCF leadership.

B. Prohibited Use:

AI must not be used to generate or manipulate content that could mislead, misinform, or misrepresent the organization or its stakeholders.

AI tools must not be used to process or store sensitive, confidential, or personal/organization identifiable information (PII) unless explicitly authorized and compliant with data protection policies. (Do not use identifying information like, name, organization name, tax id number).

Users must not rely solely on AI – generated outputs for decisions involving legal, financial, or strategic matters without appropriate human oversight.

X. Transparency and Accountability:

When AI – generated content is used in official communications or reports, users must review and verify the accuracy and appropriateness of the content.

Users are responsible for ensuring that AI use aligns with the organization's mission, values, and ethical standards.

XI. Training and Monitoring:

Staff and volunteers will receive guidance on appropriate AI use and potential risks. See appendix for suggested AI tools. This list is subject to change as more information on privacy and protection is developed with various platforms.

The organization reserves the right to monitor AI usage to ensure compliance with this policy.

Misuse of AI tools may result in disciplinary action, including revocation of access, termination of service, or legal consequences.

XII. Cell Phone/Camera Policy

Overview

Cell phones, smartphones, cameras, and other electronic devices are an integral part of today's mobile society; however, as a member of the Foundation. It is imperative to use such devices responsibly to ensure the protection of all private information.

Barring any legal precedent, willful violations of this policy will warrant appropriate disciplinary action and could lead to termination of employment, and/or civil or criminal penalties.

Objectives of Device Regulation

The enforcement of this policy seeks to:

- Establish clear, guiding principles regarding cell phones, smart phones, cameras, and any other electronic device capable of recording information in any manner may be used.
- Protect the information entrusted to CKCF and its affiliates by its donors, fund advisors, volunteers and the like, such as Personal Financial Information (PFI), Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), and Individually Identifiable Health Information (IIHI), Health Insurance Portability and Accountability Act (HIPAA) information, and other classified, sensitive and/or confidential information categories not specified herein.
- Minimize the legal risks associated with the compromise of protected information to CKCF, its officers, employees, volunteers, review committee members, board members, contractors, vendors, and the overall accomplishment of the CKCF mission.

Policy Scope

This policy covers everyone directly affiliated with the organization, including, but not limited to: officers, directors, senior managers, employees, consultants, review committee members, board members, contractors, interns, and volunteers.

Policy

Unless expressly permitted in writing by CKCF, employees will not:

- Use their phones for any reason while driving, unless able to do so “hands – free.” Safety first!
- Use any non-issued camera or microphone to record foundation business, unless otherwise approved by senior management of CKCF.
- Use any non-issued WAP (Wireless Application Protocol) device or other device to allow internet access while using CKCF issued property. Caution all device users to be aware of non-protected access points when using apps with CKCF software.

Employees will be given a phone number that can be shared publicly and used to contact them directly.

XIII. Training and Support

All users will receive onboarding and periodic training on secure technology use.
IT support is available for troubleshooting and guidance on approved platforms.

IX. Prohibited Communications

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing
- Derogatory to any individual or group
- Obscene, sexually explicit or pornographic
- Defamatory or threatening
- In violation of any license governing the use of software
- Engaged in for any purpose that is illegal or contrary to CKCF policy or business interests

Printed materials shared at in person meetings, such as in item IV above, must be returned to the CKCF staff or board chair in attendance prior to the end of the meeting to maintain privacy and confidentiality.

X. Policy Violations

Violations of this policy may result in disciplinary action, including revocation of access, termination of employment or volunteer service, and legal action if warranted.

XI. Acknowledgment

All users must sign an acknowledgment form (electronically or with ink) confirming they have read, understood, and agree to comply with this policy.

I further acknowledge responsibility to seek guidance from staff in instance of policy compliance questions. Technology based products used for CKCF and its affiliates may have help desks that may be sought for direction and are a resource. User guides and other materials for use and proper functionality are available on their product/software sites. If you need assistance, you can reach out to CKCF staff, plus see appendix.

Appendix

Boardable Helpful Tools:

- Board Member Boardable Academy: board members how to get started in Boardable.
- User Term Consent
- Boardable Tour Video (4 minute video)
- Admin Training Dashboard - Video Tutorials
- Admin Resource Guide
- Admin Getting Started Guide
- Admin First Meeting Toolkit
- The Help Center

Boardable Security: Boardable is designed with role-based permissions, document access restrictions, and centralized administrative controls (along with integration to Microsoft, Google, and Dropbox). We support and encourage two-factor authentication. These tools can help reinforce security. You can find additional detail here: **Boardable Security Sheet**

Foundant Technology – Csuites

- Overview of CSuites Software
- Resources
- Trust and Security Center
- Product Roadmap

Community Force (Grant and Scholarship Review Platforms)

- Grant Management
- Scholarship Management
- User Guides and Releases

AI Tools (staff should use CKCF issued email for account set up)

- Microsoft Co-Pilot
- ChatGPT
- Canva Magic Studio
- Other tools should be discussed with supervisor or CKCF leadership.