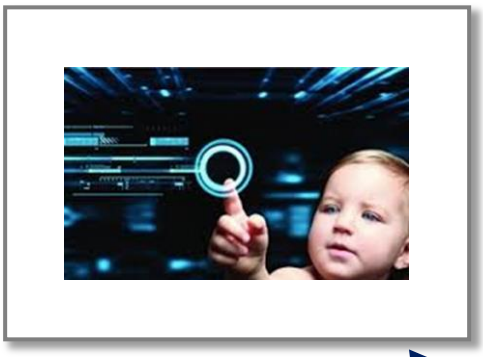


CEI

CENTER FOR EDUCATIONAL INNOVATION

Technology and Information Management Policies, Usage & Information

First Edition

Vers 1.0 6/11/15 je

Technology and Information Management

Access for users

Each user at CEI HQ that has access to the network is given a unique account and password to login to the network. Passwords should be changed every 90 days using a complex method (Pa$$w0rd). Acceptable Use Policies are in place to ensure user credentials are secure.

Virus Software and Computer Security

- Virus protection software is installed on all endpoint devices and is updated daily as new definitions are available. Virus protection software is also installed on the email gateway and updated daily to scan and prevent access to items that contain viruses.
- Battery backup devices are in place at the technology office.

Procedures for the Purchase of All Technology Items

- Any C E I personnel who wish to order any technology items or supplies must first speak with the CEI Technology Department staff.
- Request should be made via e-mail and should include a description detailing the need for the Director and/or Manager's approval, identify funding source, the location where the equipment will be installed and how it should be configured.
- Upon receipt of your request for a quote, the Technology Department will review the request and advise you if the request is the best suited for your needs.

E-Mail Accounts – Requesting a New Account

- Any individual requesting a CEI and/or DOE e-mail account must agree to abide by all applicable laws, policies, regulations and procedures for the use of district technology hardware/software.
- The email format will be first initial, last name characters followed by @thecei.org.
- E-mail that needs to be saved should be either be printed in hard copy and kept in the appropriate file; or downloaded to a computer file and kept electronically or on disk as a separate file.

The retention period depends upon the subject matter of the e-mail, as covered elsewhere in this policy.

E-Mail Accounts – Problems

- Please contact CEI's technology staff at Central HQ who will review your issue and investigate and take appropriate corrective action.
- If you receive a message that your mailbox is full, please delete all unnecessary e-mails in your -Inbox, Drafts, Sent, and Deleted Items folders. Mailboxes must be cleaned regularly email (Delete Large size first).
- Please note: that if you create any new folders, these items will still count toward your storage capacity and they should be stored on your computer.

Submissions/Changes to CEI's Web Pages

- The Director of Communications e.g. Amy Shore, maintains CEI's website. All changes and additions will go through the CEI Technology Department first.
-
- The Director of Communications will close-out the request when the web page is posted or corrected.

Phones – Requesting a New Phone

CEI Managers must send an e-mail requesting a new office telephone or cell phone to the Technology Department. The e-mail should indicate if the request is a new phone or a replacement of an existing device. The requestor should specify the type of telephone that they are requesting and the reason(s) for the request. The CFO will determine if there is a need for a new/replacement device. If the CFO determines that a new/replacement device is warranted, the Technology Department will be contacted to order the device. All cell phone users are to notify the Technology Department for approval when leaving the country in order to avoid excessive charges.

Phones/Fax Machines – Reporting a Problem

At CEI HQ your technology representative will review your issue and investigate and take appropriate corrective action. Your technology representative will close-out the work order when the issue is resolved. If you lose a call, please contact your Technology liaison immediately so appropriate steps can be taken to secure all data.

Electronic Records

CEI has computer software that duplicates files, which are then backed-up on its servers. If you save sensitive or important records on computer disks, you should duplicate the information in an alternate format because disks are easily lost or damaged.

Deleting files and emptying the recycling bin is usually sufficient in most circumstances to get rid of a record. However, because electronic records can be stored in many locations, CEI's IT department will be responsible for permanently removing deleted files from the computer system. E- Mail records that you "delete" remain in CEI's system for about 30 days. Keep in mind, where duplicate records are involved, both copies must be destroyed/deleted.

Tangible Records

Tangible records are those in which you must physically move to store, such as paper records (including records printed versions of electronically saved documents), photographs, audio recordings, advertisements and promotional items. Active records and records that need to be easily accessible may be stored in CEI's office space. Inactive CEI records should be relocated to the storage facility at CEI headquarters.

CEI obsolete records should be destroyed by shredding or some other means that will render them unreadable. If you have a record that you do not know how to destroy, such as a photograph, compact disk, or tape recording, ask the advice of CEI's Technology Manager.

CEI
Internet Acceptable Use and Safety Policy

The Center for Educational Innovation (CEI) may be provided internal access to the Internet, to the Department of Education's (DOE), and Other Internet Systems (as provided through Federal and State funded grants for its employees, and other authorized CEI agents), collectively referred to as "**users**" for educational and business purposes.. This Internet Acceptable Use and Safety Policy ("**policy**") governs all electronic activity of users using and accessing the Internet systems via computer, tablet, smartphone, etc., including e-mail and CEI/school/district-provided access to the Internet, and applies to the use of the Internet Systems both on and off CEI property.

Principles of Acceptable and Safe Internet Use General

Internet access and e-mail provided by/to CEI are intended for the business of CEI.

Monitoring and Privacy

Users have no right to privacy while using the CEI Internet System. CEI Management, in some cases, can monitors users' online activities and reserve the right to access, review, copy, store, or delete any electronic communications or files. This includes any items stored on CEI -provided devices, such as files, e-mails, cookies, and Internet history.

CEI reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent with applicable law. CEI will fully cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through Internet Systems.

Prohibited Uses of the CEI's Internet Systems

Users may not engage in any of the activities prohibited by this policy when using or accessing CEI's Internet System.

If a user is uncertain whether behavior is prohibited, he or she should contact their supervisor or other appropriate CEI personnel. CEI reserves the right to take immediate action regarding activities that:

- create security and/or safety issues for CEI employees;
- expend CEI resources on content the CEI determines lacks legitimate organization or business purpose or that CEI determines are inappropriate;
- can cause harm to others, damage to their property or CEI property;
- can gain or attempt to gain unauthorized access to the CEI's Internet System, or to any third party's computer system;
- use CEI's Internet System for personal business purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities.

Protection of Personally Identifiable & Confidential Information*

The Family Educational Rights and Privacy Act (**FERPA**) prohibit CEI officials from disclosing personally identifiable information (**PII**) from education records of students and families to third parties without parental consent.

All users of the CEI's and the DOE's Internet Systems that contain student information must comply with FERPA and New York City Chancellor's Regulation A-820, Confidentiality and Release of Student Records; Records Retention. If you are unsure about whether the activity will comply with FERPA or Chancellors

Regulation A-820, please contact the CEI's Senior Management.

Internal communications with an attorney may also be confidential. Accordingly, users should not forward or distribute such communications without first checking with the attorney. Users should ensure that e-mails that include or attach confidential information are only sent to the intended recipients.

Violations of this Policy

CEI, reserves the right to terminate any user's access to CEI Internet Systems including access to CEI e-mail at any time. If an employee violates this policy, appropriate disciplinary action may be taken. All employees must promptly disclose to their supervisor any information they receive that is inappropriate.

Limitation of Liability

CEI makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the CEI's network are to be borne by the user. CEI also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the CEI, its affiliates, or employees.

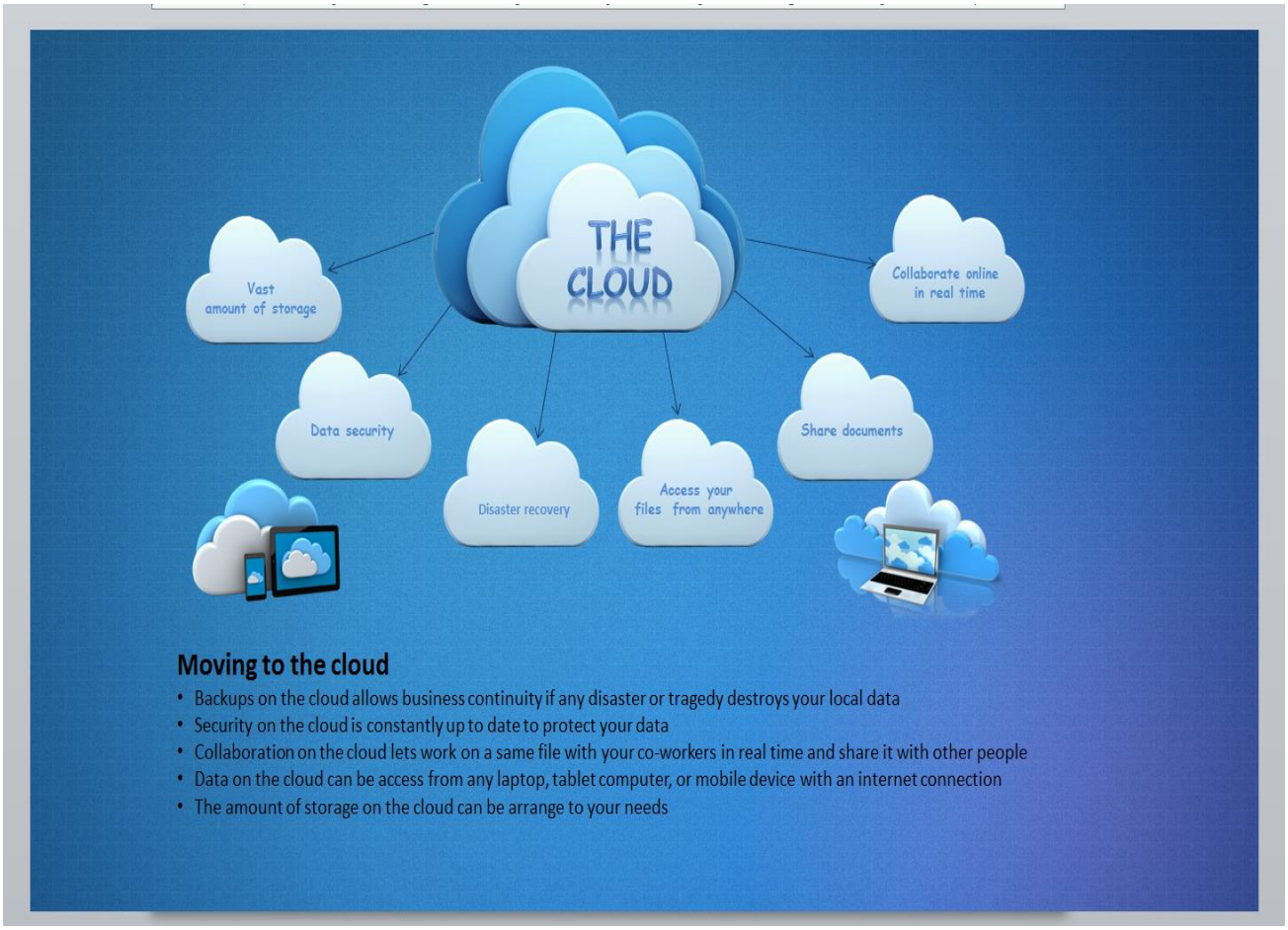
***Additional information will be available in CEI's Privacy & Security Policy**

Data Back Up

As CEI copes with the growing amount of organizational information being generated every day, CEI realized, without this data, they have no business. That's why it's so critical to now have a modern and dependable system in place to safeguard valuable business information.

Cloud backup, also known as online backup, is a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to an off-site server. The server is usually hosted by a third-party service provider, who charges the backup customer a fee based on capacity, bandwidth or number of users.

By eliminating our present tape backup system and implementing a cloud backup in July, 2014, recovery and restore solution, CEI now has an automated, safe, encrypted, daily backup and recovery system which instantly restores data regardless of location, including individual files, the most common type of data recovery.



On-site Storage of Data

Through a contract with Computer Logic, Inc., we have implemented offsite data storage for critical data for CEI Headquarters. Administrative Data such as Documents, Spreadsheets, Databases, Media files and Email are stored on local servers which are backed up on a daily basis using the latest in virtualization and replication technologies. All user data is encrypted with military-grade encryption prior to transfer. Data is stored in state-of-the-art data centers in the "Cloud."

Datto SIRIS 2 delivers the most aggressive Recovery Time Objective (RTO) of any backup, disaster recovery (BDR) and business continuity solution available today. It is the ideal solution for businesses for which downtime is not an option. SIRIS 2 offers the best protection for a business's mission-critical applications, delivered via the most robust and flexible technology on the market today.

Disaster Recovery

For use in the event of a disaster, this document identifies the computer recovery process that has been designated as backup if the functional areas are disabled. Teams and responsibilities in the event of a disaster in a Non DOE premises:

Communications Team: Director of Human Resources, Office Manager

- Notifies staff;
- Notifies Custodial Services.

Data Team: CFO, Technology Manager, Operations Manager, Contracted Vendors, CFN Technology Managers

- Coordinates support for data processing resources at the main data center and designated;
- Notifies Insurance Carrier(s).

Disaster Recovery Plan

On-site - In the event of a disaster, the Technology Managers, now Cristian Soriano and Joe Eaione will organize the disaster teams and implement the assignment of recovery tasks to the teams.

The following recovery plan will be implemented and followed until computer services normally provided by CEI staff is restored.

- Those users required to process payroll will be given priority over all other users.
- Normal financial daily operations such as p/o, receipt, and check processing will be allowed access data/recovery information's "hot site".
- All other non-essential operations will cease until normal operations are restored.

Off-site - In the event of a disaster, the appropriate personnel in the DOE will organize the disaster teams and implement the assignment of recovery tasks.

Testing the Data Recovery Plan

A test of the Disaster Recovery Plan is conducted periodically to ensure that all elements of the plan are feasible, compatible and effective. A necessary objective of the test is to minimize interference and interruption of normal operations, while providing a thorough assessment of the planned capabilities to respond to disaster.

To be used when "lending" tablets to school personnel.

IPAD (or Tablet) USER AGREEMENT

In order to effectively deliver professional development to principals and school staff, it is sometimes necessary to provide principals with an iPad. The iPads, for the purposes of observation and evaluation as well as overall instructional improvement, are made possible by the USDOE TIF awards to The Center for Educational Innovation-Public Education Association (CEI).

CEI retains sole right of possession of the iPad and related equipment. The iPad will be issued in accordance to the guidelines set forth in this document. CEI retains the right to collect and/or inspect the iPad at any time and to alter, add or delete installed software or hardware.

It is the user's responsibility to maintain the iPad condition and operation on a daily basis. In the event that the iPad is inoperable, CEI has a limited number of spare iPads for use while the iPad is repaired or replaced. This agreement remains in effect for the hot spare. A hot spare will be provided given the inoperable iPad is returned to CEI with all packaging and accessories, and that a hot spare is available. The availability of a hot spare is a courtesy not an expectation.

Report any and all damage, malfunction or loss to CEI. CEI will determine necessary action. All iPads are covered by a manufacturer's extended warranty as well as an additional insurance policy. The warranty covers manufacturer's defects. The insurance covers accidental damage from liquid spills, power surges, drops, falls, collisions, vandalism, flood, fire, smoke, wind, and earthquake, as well as damage to batteries and ac adapters. Insurance does not cover loss, negligence, abuse or theft if an iPad is lost or damaged by neglect or abuse; it is the user's financial responsibility to replace the iPad at a price of approximately $625. If an iPad is damaged, CEI will work with the user, Apple, and the insurance company to determine if it is a warranty or insurance claim incident. User is not allowed to take matters into their own hands, doing so will void warranty and all costs associated with replacement or repair will be at the personal cost of the user.

Data usage on the iPad is limited to 3 Gigabytes per month. Data usage occurs anytime the internet or applications that require internet usage are being used. User can monitor their data usage in the General tab in Settings. If a user is not clear about the current data usage amount or data balance, user may contact CEI for inquiry. The user is permitted to alter or add files to customize the assigned iPad to their own working styles (i.e. System Preferences). However, the user is not allowed to make core software changes (i.e. Jailbreak). User is permitted to install software on the assigned iPad as long as it pertains to CEI program needs. CEI will not provide funding for downloaded iPad applications unless specified for use by the grant.

Do not do anything to the iPad that will permanently alter it in any way. Do not remove any serial numbers or any unique identification on the iPad. Keep the equipment clean. For example, do not eat or drink while using the iPad. Abide by CIPA when using the internet. When finished with the iPad, all relevant files must be backed up and the device must be returned to its original state or as directed by the appropriate Project Director.

I have read and concur with the above terms and conditions of the above IPAD User Agreement.

Agreed to: _____ Date: _____

School: _____

Center for Educational Innovation
28 West 44th Street, New York, NY 10036-6600
Phone: 212.302.8800 Fax: 212.302.0088

USE OF OFF-SITE EQUIPMENT

Mr. Fliegel:

Thank you for allowing me to take the following equipment off site from CEI.

Item	Serial Number	Attachments	Condition

I will return the above equipment available to CEI personnel when requested. I agree to be responsible for the designated equipment while it is in my possession and to return it upon request and assure it will be returned in working condition upon my separation from CEI.

If any item(s) is/are lost, stolen, destroyed or otherwise rendered inoperative I agree to reimburse CEI for the item(s) at replacement value. If any item(s) is/are damaged, I agree to pay for the repair(s).

_____ _____
(Staff Member borrowing equipment) Date

Approved: _____ _____
President Date

_____
(Date Returned)