Policy 8.1	Technology Resources Acceptable Use		
Effective Date: 2/28/12 *Last Amended Date:* 11/xx/2023	*Applicable Law/Statute:* None	*Source Doc/Dept.:* None/IT	*Authorizing I.C. Sec:* None

TECHNOLOGY RESOURCES ACCEPTABLE USE 8.1

POLICY

DuPage County's policy is to provide employees with technology resources necessary to support our goals and objectives. This policy pertains to all technology-related equipment, hardware, and software, including, but not limited to County-owned, leased, or licensed desktop and laptop computers, tablets, telephones, cell phones, copy machines, fax machines, computer systems, e-mail, other messaging software, Intranet, and Internet services, tools, and supplies.

ELIGIBILITY

• All employees, volunteers, or contractors under County Board Jurisdiction, regardless of employment status. An employee is any person hired or is subject to termination by either (1) the County Board; or (2) a Countywide Elected Official who has adopted this policy on behalf of their offices.

GUIDELINES

A. The use of County technology resources are intended primarily for County business use; however, incidental and occasional use of these systems for non-work purposes may be permitted at the discretion of the Department Head. This use is permitted at the discretion of the Department Head under the following conditions:

1. Must not result in direct costs, cause legal action against, or negatively impact the County.
2. Must not interfere with the performance of work duties.
3. Must not cause a noticeable impact or change to operational infrastructure systems, noticeably consume resources, incur support, or otherwise adversely impact the functioning of essential operations.
4. DuPage County reserves the right to monitor personal use to ensure compliance with all policies and to determine whether or not it is considered “Incidental Use” at the County’s sole discretion.

B. County employees shall have no expectation of privacy regarding their use of County technology resources. The County reserves the right to access any and all information, including files and e-mail stored on the County network or any County equipment. For the protection of the County and workforce members, the County at any time may examine DuPage County technology or information resources or intercept, monitor, review, and share data with authorized personnel and law enforcement (if necessary). Users are reminded that even deleted information may also be retrieved.

C. All County employees are expected to conduct themselves honestly and appropriately when using County technology resources. In doing so, employees are expected to respect any laws, including the Freedom of Information Act, copyrights, software licensing rules, property rights and the privacy of others. The County's computer system must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Examples of this include:

1. Copying and sharing images, music, movies, or other copyrighted material using P2P (peer to peer) file sharing or unlicensed CDs and DVDs.
2. Posting or plagiarizing copyrighted material.
3. Downloading copyrighted files which employee has not already legally procured.
4. Software without a valid license or from an unapproved source.

D. Employees are expected to exercise good judgment regarding appropriate use of County technology resources and equipment and adhere to any safety guidelines related to a piece of equipment.

E. Employees are expected to limit the use of personal electronic devices and other personal equipment for non-work-related purposes during working hours. Any limited use will be at the discretion of the Department Head.

F. Employees may not blog, or use other forms of commonly known social media or technology, using County equipment on the Internet/Intranet during their designated work schedule unless specifically authorized by the Department Head as part of the employee's position. DuPage County reserves the right to discontinue employee access to County equipment if an employee is found to have posted content that is deemed inappropriate including, but not limited to, content which:

1. Violates any laws.
2. Is libelous or may be construed as harassment (Personnel Policy 6C: Harassment).
3. Violates any County policies, rules, standards, or requirements, including, but not limited to, the County's Ethics Ordinance and Personnel Policy 6H: Employment Ethics.
4. Is adverse to the reputation, interests, or business relationships of DuPage County.

G. Instant Messaging, defined as online chat that offers real-time text transmission over the internet, is allowed for County business communications only. Employees should recognize that Instant Messaging is an unsecure method of communication and should take necessary steps to follow guidelines on disclosing confidential data.

H. Employees may not remove County equipment from the location where the equipment is assigned, with the exception of cellular devices, equipment installed in vehicles, or equipment intended to be used in the field unless otherwise authorized by the Department Head and Information Technology. Once approved, Information Technology must be notified in order to update their records. Upon separation, all technology resources must be returned to the Information Technology department.

I. County employees shall not install, remove, or otherwise modify any hardware or software without written approval of their Department Head and IT Department.

J. Employees will be issued one desktop or laptop for their use. Employees will not be allowed multiple desktops or laptops for their sole use unless authorized by their Department Head and the CIO. Kiosks or computers for use by multiple employees are exempt from this requirement.

K. Employees are responsible for ensuring the protection and security of assigned County technology resources. Technology resources must be secured when not in use. Missing equipment must be reported to the Department Head, Security Department, and Information Technology Department immediately.

1. Laptop locks and cables must be used to secure laptops when in a non-secured area.
2. Mobile devices must be kept out of sight when not in use.
3. Care must be given when using or transporting devices in busy areas.
4. As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.
5. The County may use remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.

NETWORK USE GUIDELINES

A. The DuPage County Information Technology department shall be the sole provider of designs, specifications, operations, maintenance, and management of all network infrastructure and equipment including, but not limited to, switches, routers, firewalls, wireless access points and the wired/wireless local area network, with the exception of departments that have their own network staff.

B. With the exception of the IT Department, and other employees approved by their Department Head or Elected Official and the CIO, no Employee shall be granted administrative rights to any Network equipment.

C. Remote access to the County systems shall only be allowed via County approved software and hardware. Remote access systems are to be used in the same manner as computer systems within the County offices and are subject to the same policies. Employees shall ensure reasonable physical security is maintained for the computing systems used for remote access.

D. Non-County provided equipment is expressly prohibited on the County's network.

COMPUTER USE GUIDELINES

A. Employees will safeguard login identifications and passwords. Any suspected password compromise will be reported immediately to the IT Department. Password and access information may not be recorded, shared, or given to anyone other than the Employee.

B. No Employee shall allow non-County IT Staff to assume unsupervised control of a computer or application to which you have logged in with your username.

C. All Employees are responsible for logging out of or locking their workstation before they leave the office/desk unattended so that unauthorized persons cannot see, read, or take/copy confidential data. Contact the IT Department for procedures concerning the automatic locking of workstations.

D. No Employee shall be granted a primary login with administrative rights to their workstation, except as approved by their Department Head or Elected Official and the CIO.

E. No personal data shall be stored on County Servers. This includes, but is not limited to, documents, pictures, music, and video files. Information Technology reserves the right to remove any personal documents, pictures, music, or video files without warning. Findings shall be reported to the employee's supervisor.

F. No confidential data shall be stored on any local or removable media devices that are not encrypted with County approved encryption software.

G. Data stored locally on desktops and laptops is not backed up by the IT Department. No County business-related data shall be stored on any local hard drives. The IT Department will provide training to ensure that data is being stored in the correct location.

H. No County data shall be sent using personal or non-County provided email.

I. No County data shall be shared using non-County provided storage unless required by an outside vendor and with the approval of the Department Head or Elected Official.

J. Employees are prohibited from modifying County-owned technology without approval from their Department Head and the IT Department, or an Elected Official. Modifications that could impact the County network, desktop computing devices, and other computer systems are strictly prohibited. The modifications include, but are not limited to, software installation and configuration changes. Installation of non-business-related software is prohibited.

K. The Internet is a network of interconnected computers over which the County has very little control. Employees should recognize this when using the Internet and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. Employees must use the Internet at their own risk. The County is not responsible for any information Employees view, read, or download from the Internet. The County may use software to filter offensive, sexually explicit, inappropriate, or non-business-related sites.

L. Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media, such as internet radio stations or internet videos, is allowed for job-related functions only.

M. Excessive use, as defined by the IT department, of County bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low County-wide usage. If contacted by the IT department with regards to the excessive use of bandwidth employees will follow the instructions of the IT department.

N. Using County-owned or County-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

O. No County-owned or County-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions include, but are not limited to, the following:

1. Unauthorized port scanning, defined as systematically scanning a computer's ports.
2. Unauthorized network hacking, defined as any technical effort to manipulate the normal behavior of network connections and connected systems.
3. Unauthorized packet sniffing, defined as the act of capturing packets of data flowing across a computer network.
4. Unauthorized packet spoofing, defined as creating internet protocol packets with a false source IP address.

5. Unauthorized Denial of Services, defined as a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users.
6. Unauthorized wireless hacking, defined as accessing wireless networks by defeating the security devices within that wireless network.
7. Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system.
8. Acts of Terrorism.
9. Identity Theft, defined as the fraudulent acquisition and/or use of a person's private identifying information.
10. Spying.
11. Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes, except as authorized by a Department Head or Elected Official for the purpose of County business, e.g. criminal case investigations.
12. Downloading, storing, or distributing copyrighted material without proper licensing.

The County will take all necessary steps to report and prosecute any violations of this policy.

EMAIL USE GUIDELINES

A. County employees shall identify themselves accurately and completely when corresponding with others by means of telephone, e-mail, Intranet, or Internet and shall not send any unsolicited mass e-mails or e-mails used for solicitation purposes with the exception of County-supported charities.

B. Email accounts will be set up for each Employee determined to have a business need to send and receive County email. Accounts will be set up at the time a new Employee starts with the County or when a promotion or change in work responsibilities for an existing Employee creates the need to send and receive mail.

C. When an Employee leaves the County or their email access is officially terminated for another reason, the IT Department will disable the Employee's access to the account by password change or by disabling the account. If necessary, and at the request of the Department, the IT Department will either provide access to the former Employee's account to another Employee or will forward the emails sent to that account to another Employee. An Out of Office response should be set up to notify any senders that the County no longer employs the Employee.

D. No less than sixty (60) days after an Employee terminates employment with the County, the email account will be unlicensed and hidden in the system. Email will be removed from the system per the email retention policy. It is the responsibility of the Employee's Department Head or Elected Official or their designee to remove any Records per the State of Illinois Records Retention Act, or other applicable laws or statutes, from the email system and store them in another location. If the email account needs to be

retained longer than sixty days, the Department Head or Elected Official, or their designee, must notify the IT Department in writing.

E. Employees must use the County email system for all County business-related emails. Employees are prohibited from sending County business emails from a non-County provided email account.

F. When using a County email account, email must be addressed and sent carefully. Employees should keep in mind that the County loses any control of email once it is sent externally to the County network. Employees must take extreme care when typing in email addresses, particularly when email auto-complete features are enabled, using the "reply all" function, or using distribution lists to avoid inadvertent information disclosure to unintended recipients. Careful use of email will help the County avoid unintentional disclosure of private, sensitive, or non-public information.

G. Retrieval, interception, or reading of an email or other electronic messages not addressed to the Employee, unless expressly authorized by the Department Head or by the message's original recipient, is prohibited.

H. Limited Personal usage of the County email systems is permitted at the discretion of the Department Head, Chief Administrative Officer, or Elected Official as long as such usage does not negatively impact the County computer network and/or such usage does not negatively impact the employee's job performance. Conducting non-County related business emails from a County email account is prohibited.

I. The County email systems shall never be used for: spamming, harassment, issuing threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.

J. The County makes the distinction between the sending of mass emails and the sending of unsolicited emails (SPAM). Mass emails may be useful and are allowed as the situation dictates. Sending of SPAM emails is strictly prohibited. Mass emails must have the following characteristics. Emails sent to County employees or persons who have already inquired about the County's services are exempt from the below requirements.

1. The email must contain instructions on how to unsubscribe from receiving future emails. Unsubscribe requests must be honored immediately.
2. The email must contain a subject line relevant to the content.
3. The email must contain contact information, including the physical address of the sender.
4. The email must not contain intentionally misleading information. This excludes emails generated by the Information Technology department for the purposes of security training.

K. Employees are prohibited from forging email header information or attempting to impersonate another person using the County Email system.

L. Email is an unsecured method of communication and thus, information that is considered confidential, Personally Identifiable Information, or HIPAA information may not be sent via email, regardless of the recipient, without proper encryption.

M. It is County policy not to open email attachments from unknown senders, or when such attachments are unexpected. Suspicious emails or attachments should be forwarded to IT Security Department for review.

N. Email systems were not designed to transfer large files, and as such, emails should not contain attachments of excessive file size.

O. The County uses email as an important communication medium for County business operations. Employees who use the County email system are expected to check and respond to emails consistently and promptly during business hours. Email content reflects on the County and must be professional and courteous.

P. Email signatures (contact information at the bottom of each email) must be used for emails sent externally and should be used for emails sent to other employees within the County email system. Employees must keep signatures professional in nature. At a minimum, the signature must identify the County, the sender's name, and their Department.

Q. The County requires the use of an Out of Office message if the employee will be out of the office for the entire business day or more. The message should notify the sender that the employee is out of the office and who the sender should contact if immediate assistance is required.

R. Employees should be advised that the County owns and maintains all legal rights to its email system and network, and thus any email passing through these systems is owned by the County, and it may be subject to use for purposes not anticipated by the employee. Email may be backed up, copied, retained, or used for legal, disciplinary, or other reasons. Additionally, emails sent to or from the County may be considered public record and, therefore, subject to the Freedom of Information Act (5 ILCS 140/1 et seq.).

S. Accessing the County's email system from a non-County device without the permission of an Employee's supervisor is prohibited. If the County provides the Employee a smartphone, then permission is implied.

T. The County requires the use of email disclaimers and attaches email disclaimers on every original outgoing external email sent from County Board Departments. An email disclaimer is appended to the bottom of outgoing email messages and is intended to

notify recipients of any limitations on the email content. For example, that content may be subject to public inspection as part of the Freedom of Information Act.

U. Emails that are or may be constituted as "Records" per the State of Illinois Records Retention Act must be retained as per the regulations in that act. Each Department's Application for Authority determines what constitutes a Record to dispose of local records. These records should be retained outside of the email system.

V. Employees are encouraged to delete non-record emails periodically when the email is no longer needed for business purposes, however, Employees are strictly prohibited from deleting an email in an attempt to hide a violation of this or another County policy, or where the deleted email is a "record" as defined by the Illinois Record Retention Act. Email must not be deleted when there is an active investigation or litigation where that email may be relevant.

CELLPHONE AND WIRELESS DEVICE USE

The County will provide cellphones to employees where an employee is required, at the sole discretion of the Department Head, to have a cellphone to conduct County business. Any cellphone equipment provided will be limited to equipment that is provided at minimal cost by the current contracted wireless carrier. Exceptions will be made on a case-by-case basis and only if a special accommodation is needed. The following guidelines apply to all devices used to access the County's e-mail system.

A. Employees shall not download and/or save sensitive, confidential, or inappropriate information to their wireless devices unless the devices are encrypted with County approved encryption software and/or are password protected.

B. Employees are responsible for locking and securing their wireless devices. Please contact the IT Department for procedures regarding securing wireless devices.

C. All wireless devices that access the County's e-mail system must have the ability to be disabled remotely.

D. Installation of non-business-related applications or software that results in any cost to the County is prohibited.

E. Lost phones must be reported immediately to the Department Head or Elected Official, Security Office, and the IT Department.

SECURITY AWARENESS

Technology and information resource users are required to complete the mandatory security training and are requested to review any additional material when made available. At a minimum, this will occur at hire and annually thereafter.

Inappropriate use of County-owned equipment may result in disciplinary action, not to exclude termination. (Personnel Policy 10.1: Disciplinary Guidelines)

REPORTING OF A SECURITY INCIDENT

If a security incident or breach of any security policies is discovered or suspected, the Employee must immediately notify his or her Department Manager or Elected Official, the Security Department and/or the CIO or their representatives. Employees must treat a suspected security incident as confidential information. Employees must not withhold information relating to a security incident or interfere with an investigation. Incidents which require notification are:

A. Suspected compromise of login credentials (username, passwords, etc.).

B. Suspected virus/malware/Trojan infection.

C. Loss or theft of any device that contains County information.

D. Loss or theft of ID badge or keycard.

E. Any attempt by any person to obtain the user's password over the telephone or by email.

F. Any other suspicious event that may impact the County's information security.