Policy 8.1	Technology Resources Acceptable Use		
Effective Date: 2/28/2012 *Last Amended Date:* 4/8/2025	*Applicable Law/Statute:* Illinois Information Security Improvement Act (20 ILCS 1375/5-30) Personal Information Protection Act (815 ILCS 530)	*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 under County Board jurisdiction, regardless of employment status. To the extent that this policy constitutes a term or condition of employment which is required to be bargained under any collective bargaining agreement, employees covered by such an agreement shall not be subject to the terms of this policy until such time as the bargaining agreement is amended or the policy terms are agreed to by the unit.

GUIDELINES

A. The use of County technology resources is 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 under the following conditions:
   a. Must not result in direct costs, cause legal action against, or negatively impact the County.
   b. Must not interfere with the performance of work duties.
   c. Must not cause a noticeable impact or change to operational infrastructure systems, noticeably consume resources, incur support, or otherwise

adversely affect the functioning of essential operations.

d. DuPage County reserves the right to monitor personal use to ensure compliance with all policies and determine whether 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. The County may at any time examine technology or information resources, or intercept, monitor, review, and share data with authorized personnel and law enforcement if necessary.

C. All County employees must use County technology resources in a manner that complies with applicable laws and policies. This includes adhering to the Freedom of Information Act, copyright and software licensing rules, property rights, and privacy protections. 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:

a. Copying and sharing images, music, movies, or other copyrighted material using P2P (peer to peer) file sharing, or unlicensed CD’s and DVD’s;
b. Posting or plagiarizing copyrighted material;
c. Downloading copyrighted files which the employee has not already legally procured;
d. Software without a valid license or from an unapproved source.

D. Employees are expected to exercise good judgement 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.

G. 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:

a. Violates any laws;
b. Is libelous or may be construed as harassment (Personnel Policy 7.4: Harassment);
c. Violates any County policies, rules, standards, or requirements, including, but not limited to, the County’s Ethics Ordinance and Personnel Policy 9.1: Employment Ethics;

d. Is averse to the reputation, interests, or business relationships of DuPage County.

H. Instant messaging such as Microsoft Teams is allowed for County businesses communications only.

I. Employees may not remove County equipment from the location where the equipment is assigned, except for 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.

J. Employees shall not install, remove, or otherwise modify any hardware or software without written approval of their Department Head and Information Technology.

K. 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 Information Technology. Kiosks or computers for use by multiple employees are exempt from this requirement.

L. 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 immediately.

a. Laptop locks and cables must be used to secure laptops when in a non-secured area;
b. Mobile devices must be kept out of sight when not in use;
c. Care must be given when using or transporting devices in busy areas;
d. Generally, 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.

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, except for departments that have their own network staff.

B. With the exception of the Information Technology Department, and other employees approved by their Department Head and the Chief Information Officer (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 must safeguard login identifiers and passwords. Any suspected password compromise must be reported immediately to the Information Technology 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 Information Technology 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 locking or logging out of their workstation before they leave the office/desk unattended.

D. No employee shall be granted a primary login with administrative rights to their workstation, except as approved by their Department Head or the Chief Information Officer.

E. No personal data shall be stored on County servers. This includes but is not limited to, documents, pictures, music, and video files. The Information Technology Department 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 information shall be stored on any local or removable media devices that are not encrypted with County approved encryption software.

G. No County business-related data shall be stored on any local hard drives. The Information Technology Department will provide training to ensure that data is being stored in the correct location

H. 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.

I. Employees are prohibited from modifying County-owned technology without approval from their Department Head and Information Technology Department. These modifications include, but are not limited to, software installation, hardware installation, and configuration changes. Installation of non-business-related software is prohibited.

J. While the County permits limited personal Internet usage, the County assumes no responsibility for any content that the employee may view or read that they find offensive. The County may use software to filter offensive, sexually explicit, inappropriate, or non-business-related sites.

K. Streaming media, such as internet radio stations or internet videos, is allowed for job-related functions only, subject to the approval of the Department Head and/or Information Technology Department.

L. Excessive use, as defined by the Information Technology Department, of County bandwidth or other computer resources is not permitted. Bandwidth-intensive tasks that may degrade network capacity or performance such as large file downloads or uploads or streaming audio or video should be coordinated with the Information Technology Department. If contacted by the Information Technology Department with regards to the excessive use of bandwidth employees will follow the instructions of the Information Technology Department.

M. Utilizing county-owned or county-provided computer systems to bypass any established security, authentication, or user-access controls is strictly prohibited. Any deliberate attempt to circumvent these security measures, including efforts to escalate privileges, is expressly forbidden.

N. Illegal activities using County-owned or County-provided computer systems are prohibited. Such actions include but are not limited to:

a. Unauthorized port scanning, defined as systematically scanning a computer's ports;
b. Unauthorized network hacking, defined as any technical effort to manipulate the normal behavior of network connections and connected systems;
c. Unauthorized packet sniffing, defined as the act of capturing packets of data flowing across a computer network;
d. Unauthorized packet spoofing, defined as creating internet protocol packets with a false source IP address;
e. 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;
f. Unauthorized wireless hacking, defined as accessing wireless networks by defeating the security devices within that wireless network;
g. Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system;
h. Acts of Terrorism;
i. Identity Theft, defined as the fraudulent acquisition and/or use of a person's private identifying information;
j. Spying;
k. Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes, except as authorized by a Department Head for the purpose of County business.
l. Downloading, storing, or distributing copyrighted material without proper licensing.

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 department approved emails.

B. Email accounts will be set up for each employee determined to have a business need to send and receive County email.

C. 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.

D. 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.

E. Limited personal usage of the County email systems is permitted at the discretion of the Department Head 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 from a County email account is prohibited. No County data shall be sent using personal or non-County provided email.

F. The County email systems may not be used for the following, which may include but is not limited to spamming, harassment, issuing threats, solicitations, chain letters, or pyramid schemes.

G. 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 with the approval of the Department Head or the Information Technology Department. 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:

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

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

I. Information that is considered confidential, Personally Identifiable Information (PII), or Health Insurance Portability and Accountability Act (HIPAA) information may not be sent via email to an external recipient without proper encryption applied.

J. Suspicious emails or attachments should be forwarded to the Information

Technology Department for review.

K. 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.

L. 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. 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.

M. Accessing the County's email system from a non-County device without the permission of an employee's supervisor is prohibited.

N. 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.

O. 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 GUIDELINES

The County will provide cellphones to employees where an employee is required, in the sole discretion of the Department Head, to have a cellphone to conduct County business. 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 when not in use. Please contact the Information Technology Department for procedures regarding securing wireless devices.

C. Purchases from the app store without prior authorization of the department head is prohibited.

D. Lost phones must be reported immediately to the Department Head, the Security Department, and the Information Technology 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 annually per Illinois State Law (20 ILCS 1375/5-30) Illinois Information Security Improvement Act.

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 Head and the Information Technology Department. 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 can include:

- **A.** Suspected compromise of login credentials (username, password, 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.

POLICY VIOLATIONS

Consistent with the County's policy regarding all County workplace procedures, the following conduct is strictly prohibited in relation to Technology Resources:

- **A.** Engaging in fraud, misrepresentation, or providing false information to the County.
- **B.** Failure to comply with employees' obligations under this policy to include Network Guidelines, Computer Use Guidelines, Email Use Guidelines, and Cellphone and Wireless Device Use Guidelines.
- **C.** Knowingly using County-owned or County-provided computer systems or equipment for activities that are considered illegal under local, state, federal, or international law.

Employees who engage in such conduct will be subject to discipline, up to and including discharge.