GENESEE COUNTY
MICHIGAN

02.003: Technology Use Policy

Effective: xx/xx/xxxx – RES-XXXX-XXX

Purpose:

The purpose of this policy is to establish guidelines for the appropriate use of County-provided networks, computers, internet access, and devices, as well as personally owned devices used for County business. It aims to ensure secure, ethical, and efficient use of network resources and devices to promote productivity, protect sensitive data, and maintain the County's cybersecurity standards.

Authority and Responsibility:

This policy is authorized by the Board of Commissioners. The Chief Information Officer (CIO) is responsible for its implementation and oversight. The IT Department monitors compliance, provides training, and supports secure internet and device use.

Application:

This policy applies to all employees, contractors, and authorized users (hereafter referred to as "users") who use County-provided or approved personal devices, including computers, laptops, and devices. It governs the use of County network resources, data access, and software applications both on and off County premises.

Contents

Definitions:

1. **User(s):** Any elected official, appointee, employee, contractor, vendor, volunteer or other authorized individual who accesses County systems, networks, devices, or data in the course of their work or services provided to Genesee County.
2. **Supervisor:** An employee's direct manager or departmental leader responsible for approving requests and ensuring compliance with County policies. In the case of non-employee users, this term refers to the employee responsible for overseeing the user's activities for the county.
3. **County-Approved:** Refers to tools, platforms, or processes that have been evaluated, authorized, and designated as acceptable for use by the County's IT Department.
4. **County-Issued:** Devices, tools, or resources provided to users by Genesee County, including but not limited to laptops, desktops, phones, software, and email accounts, for the purpose of performing job responsibilities. The County's IT Department is responsible for procuring and tracking.
5. **Access credentials:** Any username, password, multi-factor authentication method, badge, keycard, token, certificate, or other mechanism used to authenticate identity or authorize access to County systems, applications, or facilities.
6. **Mobile Devices:** Portable computing devices capable of storing, processing, or transmitting data without a fixed physical connection. This includes smartphones, tablets, and similar handheld devices that can connect to County systems, networks, or resources, whether County-issued or personally owned.
7. **Sensitive Data:** Information classified as confidential or critical to County operations. This includes Personally Identifiable Information (PII), health records, legal documents, financial data, tax records, court records and other information that, if disclosed, could harm the County, its employees, or the public.
8. **Remote Work:** Refers to a work arrangement in which users perform their job duties and responsibilities from a location outside of the county's physical offices.
9. **Hybrid Work:** Hybrid work is an employee benefit that may be granted under limited circumstances to allow employees to perform some of their duties from home.
10. **County Network:** All wired and wireless infrastructure, firewalls, VPNs, and internet connections maintained by the County.
11. **IT Department:** The department responsible for technology governance, security, and support.
12. **FOIA:** Freedom of Information Act, a federal law requiring disclosure of public records upon request.
13. **Sensitive System:** Any system storing or processing confidential or critical data, or designated as sensitive by IT.

Policy:

1. Provided Technology and User Responsibilities

a. Genesee County is committed to equipping its users with the technology and resources necessary to perform their duties effectively, securely, and efficiently. As part of this commitment, each user will be provided with a county email address, a computer, and a desk or softphone as required by their role. County-issued cell phones may be provided based on specific operational needs, determined by department requirements and approved by the Department Head. It is the County's intent to provide all users with the appropriate technology tools and resources needed to fulfill their responsibilities without requiring the use or purchase of personal technology.

b. Users must only use County-approved devices and resources to conduct County business, ensuring compliance with applicable policies, safeguarding sensitive information, and maintaining a unified standard of technology and security.

c. Users are prohibited from installing unauthorized software, applications, or browser extensions on County devices. All software requests must go through IT for approval.

d. All County-issued technology must be inventoried by the IT department and tagged with an asset ID when appropriate.

e. Technology may not be reassigned or transferred to another user without prior authorization from the IT Department.

f. All technology assigned to, or for, individuals will be returned to the IT Department upon separation or reassignment of said user.

2. County Issued Mobile Device Eligibility and Usage

a. County-issued mobile devices and related services may be provided to certain Genesee County users to conduct work related business. The user's Department Head will determine the need for a cell phone and must approve any requests prior to device issuance.

b. County issued mobile devices may be assigned to users provided that at least one of the following criteria is met. Simple convenience is not a valid criterion for issuance.

   i. The job function of the user requires considerable time outside of their assigned office or work area and it is important to the County that they are accessible during those times.

   ii. The job function of the user requires them to be accessible outside of scheduled or normal working hours.

c. County issued mobile devices are subject to monitoring and may be collected during litigation or Freedom of Information Act requests.

Acquisition and Issuance

d. All County provided mobile devices are to be acquired through the IT Department. No other department is authorized to acquire mobile devices independently.
   i. The IT Department is responsible for ordering and managing all mobile devices, service and accessories.
   ii. The cost of the mobile devices, service and accessories will be the responsibility of the user's department.
   iii. Mobile devices and service providers shall be managed through the Genesee County IT Department.
   iv. Mobile devices will use the County-managed Mobile Device Management
   v. The IT Department will provide the necessary orientation and training of new equipment.

Loss of Business Need

e. The Department Head or designee is responsible for notifying the IT department when the user no longer has a business need for a cell phone. Department Heads are responsible for notifying the IT department when the user terminates employment or contractual relationship with the County and for ensuring the user returns their cell phone and any accessories.

3. Bring Your Own Device (BYOD) Policy

a. BYOD is strictly limited to personal cell phones. The use of personal laptops, tablets, or other devices for County business is prohibited unless written authorized by the IT department is obtained. County-provided computers and devices are required for all work to ensure secure, compliant access to County resources.

b. It is important to understand that personal device use is optional and at the user's own risk. The county is not responsible for the loss, theft, or any damage caused to or by a personally owned device. In certain cases, the use of a personal device may bring the device into the scope of certain FOIA or legal requests. If you have questions or concerns, please contact the IT Helpdesk prior to connecting your personal device.

c. County business, communications, and data storage must not occur on personal devices. This includes but is not limited to scanned images, pictures or videos.

d. The IT Department may revoke or restrict personal device access to County systems if security concerns are identified.

4. Requesting Additional Technology Resources

a. If a user identifies a new technology need that is not met by their current County-issued resources:

i. **Discuss the Need with Your Supervisor:** Users must first bring the matter to their immediate supervisor. The supervisor will evaluate the request in the context of the user's job responsibilities and operational needs.

ii. **Submit a Formal Request to IT:** If the supervisor agrees that additional resources are necessary, the supervisor will assist the user in submitting a formal technology request to the County's IT department. Requests should include a clear explanation of the need, how the requested technology will enhance or support the user's duties, and any relevant supporting documentation.

iii. **IT Evaluation and Approval:** The IT department will review the request to ensure it aligns with the County's technology standards, cybersecurity requirements, and budgetary constraints. If approved, IT will provide the necessary technology or an alternative solution that meets the identified need.

iv. **See Policy:** IT Procurement Policy for more details

5. Multi-Factor Authentication (MFA) and Personal Device Use

a. As part of the County's cybersecurity program, Multi-Factor Authentication (MFA) is required to access County systems and accounts. MFA provides an additional layer of security by verifying user identity through a trusted device, such as a smartphone. This practice helps protect sensitive County data and systems against unauthorized access.

i. **Purpose of MFA on Personal Devices:** The use of a personal device for MFA is strictly limited to identity verification. This does not constitute the use of personal technology for County operations.

ii. **Separation of County Work and Personal Device Use:** MFA apps, such as DUO and Microsoft Authenticator, installed on personal smartphones are limited to authentication functions only. MFA apps do not process any data or perform any function other than confirming identity.

iii. **Security and Privacy Protections:** The County does not monitor or access any personal data on personal devices used for MFA. The MFA application operates independently and is solely used for identity verification.

6. Account Security and Password Management

a. To protect County systems, facilities, and sensitive information, all users must adhere to strict account and access credential security practices.

i. **Account Integrity:** Users must not share, duplicate, or replicate their access credentials. Each user must log in using their assigned account and ensure they are logged out when not actively using the system.

ii. **Password Confidentiality:** Passwords must remain confidential and must not be disclosed, written down in unsecured locations, or stored in an unapproved manner.

iii. **Password Complexity Requirements:** Passwords must adhere to the requirements set by County IT and will be enforced when resetting a computer account password.

i) When creating a password for a cloud-based service, use a unique password that adheres to the following criteria: a minimum of 12 characters, must include both uppercase and lowercase letters, at least one number (0–9), and one special character (e.g., @, #, $, %).

ii) It is recommended to use passphrases to create secure and memorable passwords, such as 'Gr3at!DayT@Work2026'.

iv. **Unique Password Requirements:** Users must create a unique password for each account. Reuse of passwords across multiple systems or services is prohibited.

v. **Password Management Best Practices:** Passwords should not be written down, stored on paper, or saved in unsecured locations. Users are encouraged to use a password manager approved by IT Security to securely store and manage unique passwords.

vi. **Credential Duplication:** Access credentials must not be copied, cloned, or replicated. Physical credentials (such as badges or keycards) may not be duplicated or embedded into personal devices, wearables, or third-party tools. County-managed authentication methods deployed through approved systems are permitted.

vii. **Multifactor Authentication / SSO:** When available, MFA must be enabled for all accounts. Users must notify IT if a service supports Single Sign-On (SSO) to reduce password usage and improve security.

viii. **Compromised Password:** If a user suspects their password is compromised, the users should change their passwords and notify the IT department immediately.

7. Data Protection and Classification

a. To safeguard the confidentiality, integrity, and availability of County data, all users are responsible for protecting information accessed, created, transmitted, or stored using County technology resources.

2. Data Classification

i. Departments are responsible for identifying and documenting the types and sources of confidential data they manage.

ii. Confidential data includes, but is not limited to:

i) Information protected by law or regulation (such as HIPAA, FERPA, CJIS Security Policy, or similar laws)

ii) Personally Identifiable Information (PII), Protected Health Information (PHI), Sensitive PII (SPII), or other data that could cause harm or legal liability if disclosed

iii) Any data a department designates as confidential or sensitive

iii. Users must treat all data as confidential until confirmed otherwise by their department.

3. **Handling and Storage**
   i. Confidential data must only be stored on County-managed systems or County-approved cloud services.
   ii. Users must not store Confidential data on personal devices, removable media, or unapproved third-party services.
   iii. Users must apply security controls appropriate to the data's sensitivity, including encryption and Multi-factor authentication (MFA) when available.
4. **Transmission and Sharing**
   i. Confidential data must not be transmitted via unencrypted email or messaging platforms.
   ii. Data sharing outside the County must be authorized and use secure, approved methods.
   iii. Users must verify the recipient's identity before sending Confidential data.
5. **Data Retention and Destruction**
   i. Users must comply with the County's Data Retention and Data Destruction policies when handling or disposing of data, whether physical or electronic.
   ii. Users must not delete, destroy, or dispose of data without confirming compliance with retention requirements.
   iii. Digital media and physical documents containing Confidential data must be disposed of only through County-approved processes managed or approved by the IT department
6. **Reporting and Accountability**
   i. Any suspected loss, exposure, or unauthorized disclosure of Confidential data must be reported immediately to the IT Department.
   ii. Failure to comply with data protection requirements may result in disciplinary action, up to and including termination of employment.

8. Acceptable Use

The use of email, internet, and sensitive data must align with Genesee County's policies to ensure security, efficiency, and compliance with legal and operational standards. This section outlines acceptable use for these critical resources.

a. Email Acceptable Use

7. **Official County Business**
   i. County-provided email accounts must be used for all work-related communications.

ii. Personal email accounts must never be used to conduct County business under any circumstances.

8. **Professional and Appropriate Content**

iii. Emails sent from County accounts must reflect professionalism and adhere to County policies on respect and non-discrimination.

iv. The use of County email for personal, political, or commercial purposes is prohibited.

9. **Use of County Email for Accounts and Subscriptions**

v. Users may use their County email address to create user accounts for operationally necessary services, such as accessing work related tools, subscriptions, or resources related to their job responsibilities.

vi. County email addresses may also be used to subscribe to industry-related newsletters, webinars, and professional development materials that align with County objectives.

vii. County email addresses must not be used for personal purposes, such as shopping accounts, entertainment services, or unrelated social media platforms.

10. **Email Signatures**

viii. Email signatures must be professional in appearance and follow the Genesee County Style Guide.

ix. Signatures should include accurate and up-to-date information such as the user's name, title, department, and contact details.

x. Personal quotes, slogans, or unrelated graphics are not permitted in County email signatures.

11. **Attachments and Links**

xi. Users must exercise caution when opening email attachments or clicking on links, particularly from unknown or unverified sources.

xii. If a suspicious email is received, it must be reported to IT immediately.

12. **Email Retention and Records**

xiii. The County complies with all Federal, State and Local record retention requirements including FOIA. All emails received or sent from the County email system are deemed work related and may be subject to FOIA or legal requests.

b. **Internet Acceptable Use**

13. **Work-Related Activities**

i. Internet use must be primarily for activities that support County operations, research, and job-related functions.

ii. Users may access work-related tools, resources, and training via the internet.

14. **Prohibited Activities**

iii. Accessing, downloading, or sharing inappropriate, illegal, or offensive content is strictly prohibited. This includes, but is not limited to, obscene, sexually explicit, discriminatory, or harassing material.

iv. Users must not use the internet for gambling, gaming, or conduct personal business.

15. Cybersecurity Best Practices

v. Users must avoid visiting untrusted websites and downloading unauthorized software or files to protect County systems from malware and other threats.

c. County Data Acceptable Use

16. Data Integrity and Confidentiality

i. Users are responsible for safeguarding County data, ensuring it is only accessed by authorized individuals and used for official County business.

ii. Access to sensitive data is strictly for official County use only. Any use of sensitive data outside of the scope of a user's job responsibilities is considered unauthorized and will not be tolerated.

17. Prohibited Use of Sensitive Data

iii. Unauthorized access, sharing, or use of sensitive data—including but not limited to personal information, confidential records, or proprietary County information—is strictly prohibited.

iv. Any unauthorized use of sensitive data may result in disciplinary action, up to and including termination of employment and legal action.

18. Data Storage

v. County data must only be stored on approved systems, such as County network drives or authorized cloud services.

vi. Storing County data on personal devices or unapproved platforms (e.g., personal cloud accounts) is strictly prohibited.

19. Data Sharing and Transmission

vii. Users must use secure methods to share and transmit County data, such as encrypted email or County-approved file-sharing platforms.

viii. Sharing County data via personal email, messaging apps, or unauthorized platforms is prohibited.

20. Incident Reporting

ix. Users must inform IT immediately of any unauthorized access, loss, or misuse of data to limit harm and to initiate prompt remediation.

9. Use of Artificial Intelligence (AI) Tools

Genesee Genesee County supports the responsible use of Artificial Intelligence (AI) technologies to improve productivity, service delivery, and operational effectiveness. AI tools may assist users with research, drafting, analysis, and automation. Use of AI is subject to the same security, privacy, legal, and compliance obligations that apply to all County technology resources.

a. **Approved AI Tools:** Only AI tools explicitly approved by the IT Department may be used to process County data. Approval must be obtained in writing prior to use.

b. **Prohibited Data:** Users are prohibited from providing confidential, sensitive, regulated, or personally identifiable information (PII) to any AI system that has not been approved by the IT Department.

c. **Permitted AI Usage:** Approved or public AI tools may be used for low-risk activities such as:

    i. Publicly available data

    ii. Drafting non-sensitive content (e.g., templates, forms, reports)

    iii. Summarizing publicly available policies, procedures, or regulations

d. **Human Review and Accountability:** All AI-generated content must be reviewed by the user for accuracy, completeness, and compliance prior to use or publication. Users are responsible for the content they create using AI tools.

e. **Use of AI for Decision-Making:** AI tools may not be used to make final personnel, legal, or financial decisions. Any AI-assisted recommendation must be independently verified.

f. **Accounts and Access:** Users must not create accounts on external AI platforms using their County credentials or email address without prior written approval by the IT Department.

g. **Misuse and Monitoring:** The IT Department may monitor and audit AI tool usage. Unauthorized or unsafe use of AI tools will result in loss of access and may lead to disciplinary action.

h. **Third-Party or Embedded AI Features:** AI features embedded within County-approved software must only be used after enabling any security controls or data boundaries required by the IT Department.

i. **Training Data Restrictions:** Users must not allow, authorize or directly use County data to train, fine-tune, or customize any AI system without express written approval from the IT Department

j. **Records and Retention:** AI-generated content used for official County business constitutes a County record and is subject to applicable records retention, FOIA, and legal disclosure requirements.

10. Personal Use and Misuse

a. The use of County-provided technology, internet access, and devices is intended to support the operational needs of Genesee County. While limited personal use is permitted under specific circumstances, users must ensure their activities comply with the following guidelines to avoid misuse:

Acceptable Personal Use

b. **Limited Personal Use**
   i. Incidental and reasonable personal use of County devices, internet, and personal email is allowed during breaks or non-working hours, provided it does not interfere with County operations, reduce productivity, or violate County policies.

c. **Appropriate Content and Activities**
   i. Personal use must not involve accessing, downloading, or transmitting content that is inappropriate, illegal, or offensive. This includes, but is not limited to, obscene, sexually explicit, violent, discriminatory, or harassing content.

Prohibited Misuse

d. **Excessive Personal Use**
   i. Extensive or habitual use of County resources for personal purposes is prohibited. This includes streaming non-work-related media, gaming, or conducting non-work-related business activities on County time or using County resources.

e. **Using Personal Accounts for County Activity**
   i. County data may not be stored on personal cloud storage platforms such as Google Drive, Dropbox, or iCloud.

f. **Unauthorized Use of County Resources**
   i. Users are prohibited from using County devices, software, or networks to perform work for personal gain, private businesses, or outside organizations unless explicitly authorized by County IT.

g. **Illegal or Unethical Activities**
   i. Engaging in illegal activities, such as hacking, pirating software, or accessing unauthorized systems, is strictly prohibited and will result in disciplinary action.
   ii. Users must not use County resources to promote political campaigns, solicitations, or personal causes unrelated to County business.

h. **Personal Email and Social Media Misuse**
   i. Personal email accounts and social media platforms must not be used for conducting official County business.
   ii. Users are prohibited from using County email addresses to sign up for personal services or accounts unrelated to County operations.

11. Approved Communication Channels

a. All County-related communications must occur through County-approved communication channels, including County-provided email, messaging platforms, and phones. These channels are designed to ensure secure, consistent, and transparent communication that aligns with the County's operational and regulatory requirements.

b. The use of personal email accounts, messaging apps, or personal cell phone numbers for conducting official County business is strictly prohibited. This policy ensures that all work-related communications are properly documented, easily retrievable, and compliant with legal obligations, such as FOIA requests.

c. County business communications that include sensitive or confidential data must be sent only through County-managed secure communication systems and encrypted when possible.

d. Social Media Use for County Business

i. Users must not use personal social media accounts for official County communications or to conduct County business. Posts made on behalf of the County, including responses to public inquiries or dissemination of information, must be made through County-approved social media accounts managed by designated personnel or departments.

ii. The IT Department is responsible for reviewing and facilitating the establishment of any social media account. The IT department is designated as the social media record keeper and must be given access to the username and password established to manage any County social media page.

iii. Users authorized to post on County social media channels must adhere to the County's Social Media Policy to ensure professionalism, accuracy, and alignment with County values and goals.

e. Personal Social Media Use

i. The County recognizes and respects users' right to use personal social media accounts outside of work. However, users are encouraged to act responsibly and professionally on social media platforms. Even when posting on personal accounts, users should be mindful that their statements and behavior may be perceived as reflecting on the County.

ii. While the County does not seek to restrict personal expression, users are advised to avoid content that could damage the County's reputation, disclose confidential information, or appear as an official statement from the County. If identifying as a County user on social media, users should include a disclaimer indicating that opinions expressed are their own and do not represent the views of Genesee County.

12. Data and Communication Integrity

a. All users are reminded of the importance of maintaining the integrity of data and communications. County communications may be subject to the Freedom of Information Act (FOIA) and other legal or regulatory requests. Therefore, it is imperative to only use County-approved communication methods for work-related interactions. This ensures that proper records are maintained, enabling the County to meet transparency, accountability, and compliance standards.

b. Using only County-authorized email, messaging platforms, and communication channels ensures that communications are properly archived and available for retrieval if necessary. Personal email, messaging apps, or non-County-approved communication platforms are strictly prohibited for official County business.

c. Failure to adhere to approved communication methods can lead to non-compliance with public records requests, legal obligations, and County policy. Any user found violating this section may face disciplinary action, as unauthorized communication may hinder the County's ability to meet legal requirements.

13. Remote and Hybrid Work Guidelines

a. Genesee County supports the use of remote and hybrid work arrangements where operationally feasible and in alignment with the County's goals and the user's role. These arrangements are defined and governed as follows:

Remote Work

b. Remote work refers to tasks performed outside of County buildings as part of the County's operational needs. Remote work arrangements are determined based on the role's requirements. This type of work is not discretionary but is dictated by the nature of the position and the department's needs.

i. Remote work is authorized for specific roles when working outside of County facilities is required to fulfill job duties.
ii. Users performing remote work must utilize a County-issued device and must access County resources exclusively through a County-approved Virtual Private Network (VPN) to ensure data security and compliance.
iii. Requests for remote work access or resources must be submitted by the user's supervisor directly to the IT Department for review and approval.

Hybrid Work

c. Hybrid work is an employee benefit that may be granted under limited circumstances to allow employees to perform some of their duties from home. Hybrid work arrangements are not guaranteed and are dependent on departmental approval. These arrangements must align with the role's responsibilities and the department's operational needs.

21. See Policy: Hybrid Work Policy for more details

22.

23. General Requirements

d. Users working remotely or in a hybrid capacity must maintain the same level of productivity and professionalism as expected within the office.

e. Both remote and hybrid workers must maintain a secure work environment, including a private workspace, locked screens, and physically secured County equipment.
f. VPN access is mandatory for connecting to County systems and resources.
g. Users must adhere to all County policies, including those related to data security, device use, and communication channels, while working remotely or in a hybrid environment.
h. County-owned devices must be used for all County work unless explicitly authorized otherwise.
i. Printing County documents at home is prohibited unless specifically authorized by the IT Department
j. The County reserves the right to modify or terminate remote or hybrid work arrangements if it is deemed to no longer meet operational needs or if the user fails to adhere to the outlined requirements.

14. Physical Security of Technology

To protect County-issued technology and ensure the security of sensitive data, users must adhere to the following guidelines for the physical security of devices:

Securing Devices When Not in Use

a. County-issued devices, including laptops, cell phones, and tablets, must be securely stored when not in use.
b. Devices must be locked (e.g., with a password, PIN, or biometric authentication) before being left unattended, even for short periods.

Prohibition on Leaving Devices in Vehicles

c. Users must not leave laptops, tablets, or other County-issued devices in vehicles overnight or when unattended for any extended period.
d. If transporting devices in a vehicle, users should store them out of sight, such as in a locked trunk, to reduce the risk of theft.

Unattended Technology

e. When working remotely, users must ensure that County-issued technology is never left unattended in public spaces, such as cafes, libraries, or co-working environments.
f. Users should maintain physical possession of their devices at all times while working in a non-secure location.

Awareness of Surroundings

g. Users working remotely or in public spaces must ensure that their screen is not visible to unauthorized individuals, including those nearby or via surveillance cameras.
h. Use a privacy screen or position the device to minimize visibility of sensitive information if working in areas where others might have a line of sight.

Additional Protective Measures

i. Users are encouraged to use carrying cases or protective sleeves to prevent physical damage to laptops or tablets during transport.
j. When storing devices at home, they should be kept in a secure and stable location, away from potential hazards such as pets, spills, or extreme temperatures.

15. Replacement and Reutilization

Genesee County is committed to ensuring that technology resources remain efficient, secure, and aligned with operational needs. To support this, the County has established the following guidelines for the replacement and reutilization of technology:

Technology Lifecycle Management

a. All County-issued technology, including computers, laptops, mobile devices, and peripherals, will be evaluated periodically to determine whether they meet operational performance and security requirements.
b. Devices nearing the end of their lifecycle, typically 5 years depending on usage and functionality, will be replaced proactively by the County IT Department to maintain operational efficiency and compliance with security standards.

Replacement Requests

c. Users experiencing performance issues or device failures must report them to the IT Department. Replacement requests must be approved by the user's supervisor prior to being sent to IT.
d. IT will review all performance issues and determine the appropriate manner to address the issue. This may include software cleanup, hardware and software upgrades, or even recommendations to adjust workflow. Device replacement will be considered only if the device is out of life-cycle or all other solutions have been unsuccessful.

Return Equipment to IT Department

e. All devices that are replaced must be returned to the IT Department for secure data wiping and inventory reconciliation.

f. Upon termination of employment, change in role, or issuance of a replacement device, users must return all County-issued technology to the IT Department. Failure to return equipment may result in disciplinary action or financial liability.

g. Departments must not retain or repurpose County-owned devices without explicit authorization.

Evaluation for Reutilization

h. Devices returned to the IT Department will be evaluated for potential reutilization. If a device still meets performance and security standards, it may be reassigned to another user or department.

i. Equipment unsuitable for reassignment will be decommissioned and disposed of in accordance with the County's IT asset disposal procedures.

Reassignment of Reusable Devices

j. The IT Department will prioritize reassignment of reusable devices based on departmental needs and requests.

k. Reassigned devices will be reset, updated with the latest software, and tested to ensure proper functionality before deployment.

Environmental Responsibility

l. Technology that cannot be reused will be securely recycled or disposed of in compliance with environmental regulations and County sustainability initiatives.

16. Reporting Lost, Stolen, or Damaged Devices

a. Any loss, theft, or damage of County-issued devices must be reported immediately to the IT Department and the user's supervisor. Timely reporting allows the County to secure data, track devices, and, if necessary, initiate a response to minimize security risks.

b. Costs incurred for replacement or repair, due to normal course of business, will be the responsibility of the user's department.

c. The user may be held responsible for any costs incurred for replacement or repair of equipment damaged through negligence or carelessness of said user.

d. All replacement or repair requests are to be processed by the IT Department.

17. Incident Reporting

a. To protect County systems and data, all users are required to promptly report any suspected or confirmed security incidents.

b. **Immediate Notification:** Users must immediately notify the IT Department of any suspected:

   i. Cybersecurity incidents, including data breaches, malware infections, phishing attempts, or ransomware.

   ii. Unauthorized access to County systems or accounts.

iii. Lost or stolen County-issued devices or storage media.

iv. Accidental disclosure or transmission of sensitive or confidential information.

c. **Reporting Method:**

i. Submit a Helpdesk ticket through the County IT Helpdesk system

ii. Call the IT Helpdesk at 810-257-3007 for urgent or time-sensitive issues

iii. Notify your supervisor

d. **Preservation of Evidence:** Users must not attempt to investigate, delete, remediate, or otherwise alter any suspected incident. Systems should remain powered on and connected unless otherwise instructed by the IT Department.

e. **Post-Incident Cooperation:** Users must fully cooperate with all IT Department investigations, including providing relevant information, access, or documentation as requested.

f. **Confidentiality:** Information related to incidents must not be discussed or shared with anyone other than the IT Department or authorized County leadership

18. Mandatory Cybersecurity Training

a. All users must complete annual cybersecurity training assigned by the County. This training ensures users remain informed about current security threats, best practices, and policies.

i. **Annual Training:** Annual training will be assigned near the start of each calendar year with a 30-day window to complete the training. New users granted access to County-issued technology resources will be assigned the current year's training at the time access is granted. For new users this will occur during the onboarding process.

ii. **Remediation Training:** Users may be assigned additional or remedial technology, compliance or cybersecurity training at any time throughout the year based on specific needs identified by their office or department, Information Technology or the County.

b. Completion of cybersecurity training is mandatory for all users. Failure to complete assigned training within the designated period will result in immediate termination of access to County email, network resources, and computer systems.

19. Monitoring and Compliance

a. The County reserves the right to monitor internet activity, device usage, and account access to ensure compliance with this policy and to protect the County's interests. Users should have no expectation of privacy on County-owned devices or when accessing County resources on personal devices.

20. Enforcement

a. To maintain a secure and reliable technology environment, violations of this policy will result in corrective or disciplinary actions.

b. **Potential Disciplinary Actions:** Depending on severity and intent, violations may result in:

   i. Verbal or written warnings

   ii. Temporary or permanent loss of access to County technology resources

   iii. Suspension or termination of employment

   iv. Referral for civil or criminal investigation when applicable

c. **Supervisor Responsibilities:** Supervisors and Department Heads are responsible for enforcing this policy within their areas, including notifying the IT Department of known or suspected violations.

d. **Intentional Misconduct:** Intentional, reckless, or repeated violations will be treated as serious misconduct and may result in immediate loss of access or removal from duty.

e. **Third-Party Users:** Contractors, vendors, or other third parties who violate this policy may have their access to County systems restricted or revoked and may be subject to corrective actions under the terms of their agreements, up to and including contract termination.

21. Conclusion

a. This policy ensures that Genesee County maintains a secure, efficient, and responsible digital environment. By safeguarding sensitive data, reducing cybersecurity risks, and enforcing best practices, the County promotes a productive and secure culture among its users.

b. This policy supersedes and replaces the prior Internet Use Policy, Email Policy, Cell Phone Policy, Laptop Policy, and Computer Reutilization Policy, effective immediately upon issuance.