RESOLUTION NO. 459-2019

APPROVAL OF REVISED ST. LAWRENCE COUNTY INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

By Mr. Denesha, Chair, Operations Committee

WHEREAS, the St. Lawrence County Information Technology Acceptable Use Policy has been reviewed by the Information Technology Department, and

WHEREAS, recommendations have been made for revisions to the policy, and

WHEREAS, the proposed revised St. Lawrence County Information Technology Acceptable Use Policy dated December 2, 2019 includes these recommendations,

NOW, THEREFORE, BE IT RESOLVED that the St. Lawrence County Board of Legislators approves the revised St. Lawrence County Information Technology Acceptable Use Policy dated December 2, 2019.

STATE OF NEW YORK)
) **ss:**
COUNTY OF ST. LAWRENCE)

I, Kelly S. Pearson, Deputy Clerk of the St. Lawrence County Board of Legislators, **DO HEREBY CERTIFY** that I have compared this Resolution No. 459-2019 entitled "Approval of Revised St. Lawrence County Information Technology Acceptable Use Policy", adopted December 2, 2019, with the original record in this office and that the same is a correct transcript thereof and of the whole of said original record.

Kelly S. Pearson
Kelly S. Pearson, Deputy Clerk
St. Lawrence County Board of Legislators
December 3, 2019

St. Lawrence County

Information Technology

Acceptable Use Policy

Acceptable Use Policy

Policy Contact	Rick Johnson, IT Manager
Policy Approver(s)	Board of Legislators
Related Policies	None
Related Procedures	None
Storage Location	IT Office (physical), \\slcadmin\it\policies, "Countywide_Forms"
Effective Date	December 2, 2019
Next Review Date	November 2020

Purpose

GENERAL: The purpose of the Acceptable Use Policy (AUP) is to ensure that St. Lawrence County resources are used properly, ensuring the confidentiality, integrity, and availability of information systems.

EMAIL: Email is a critical mechanism for business communications at St. Lawrence County. However, use of St. Lawrence County's electronic mail systems and services is a privilege, not a right, and therefore must be done with respect and in accordance with the goals of St. Lawrence County.

The objectives of this policy are to outline appropriate and inappropriate use of St. Lawrence County's email systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

INFORMATION: The purpose of this policy is to provide staff with clear guidance on the appropriate, safe, and legal way in which they can make use of information and IT equipment in St. Lawrence County. Staff need to be aware of the compliance required with this policy and St. Lawrence County's commitment that all reasonable organizational and technical measures are taken to safeguard its data.

INTERNET AUP: The goals of this policy are to outline appropriate and inappropriate use of St. Lawrence County's Internet resources, including the use of browsers, electronic mail and instant messaging, file uploads and downloads, and voice communications.

Scope

GENERAL: This policy applies to all users of the county network and resources, including but not limited to employees, contract workers, volunteers, interns, and any entity who conducts business on behalf of the county. These individuals will be referred to as "users." The acceptable use of computer resources, such as internet, email, and computer hardware is covered in this policy.

EMAIL: This policy applies to all email systems and services owned by St. Lawrence County, all email account users/holders at St. Lawrence County (both temporary and permanent), and all company email records.

INFORMATION: This Acceptable Use Policy (AUP) applies to the use of all information and IT equipment by St. Lawrence County staff (including temporary workers, locums, and staff contracted from other organizations). All staff should be aware of their legal obligations and internal policy in respect of information handling.

This policy should be a living document that will change as information use changes in the organization.

All employees are expected to have knowledge of at least the portions of this document that are directly related to their role within the organization.

St. Lawrence County's Internet Acceptable Use Policy applies to all employees of St. Lawrence County regardless of employment status.

This policy applies to all St. Lawrence County employees, including full and part-time staff, contractors, freelancers, and other agents who use a personally-owned device to access, store, back up, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust St. Lawrence County has built with its clients, supply chain partners, and other constituents. Consequently, employment at St. Lawrence County does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. Low Risk Information. This is defined as information that does not require special protective measures.
2. High Risk Information. This is defined as information, the loss or breach of which would substantially impair an organization and/or subject it to legal action.

Governing Laws & Regulations

The accidental or intentional disclosure of non-public County information can have serious repercussions. The County, in the event its information resources are compromised or due to county user misconduct, can face legal liability associated with the disclosure of information governed by Federal and State Laws, e.g., Health Insurance Portability Accountability Act of 1996 (HIPAA), Criminal Justice Information (CJI), and Personally Identifiable Information (PII).

Policy Statements

1. Any user who shall conduct business on behalf of St. Lawrence County and/or have access to the St. Lawrence County network must read, acknowledge, and adhere to the requirements outlined in this Policy prior to receiving or continuing access to the network.

2. If a user suspects a violation of this policy or other IT/Security policies, the user should contact the IT Helpdesk.

User Access Management

- Every user of the St. Lawrence County network must have a network user account.
- Each network account must be unique to each County User and be created by the Information Technology Department.
- Each network account will be set to disable access to the network for 30 minutes after 5 failed logon attempts.
- Network user accounts must not be shared between members of staff.
- Access to a County User's account during absence by another member of the staff must be authorized by the Supervisor/Department Head.
- Unattended computers must be logged off or protected in such a way as to protect the computer and network from unauthorized access.

Account Authentication

- All user accounts will be authenticated using passwords as a minimum.
- The minimum password length will be 12 characters.
- Each network password will be required to be changed at least every 180 days or when the password is known to have been compromised.
- Complex passwords [consisting of 3 of 4 upper case, lower case, numeric, and non-alpha-numeric] must be used.
- Passwords cannot be reused for the next 5 times.

- Passwords for network accounts must not be shared unless an authorized shared account.
- County Users must not facilitate any logon procedure with local programming such as keyboard programming or scripting or save passwords in a browser.

New Network User Accounts

- St. Lawrence County exercises a formal user registration and deregistration process for all network users, permanent and temporary.
- All new accounts are to be requested by the department head 5 days before the employee starts, with all the required access specified using the Access Authorization Form found in Countywide Forms in the Information Technology folder.
- New accounts are created with a default password which the user is required to change at first logon.
- The initial password for a network user account will only be given to the new user or department head by phone or in person.

Account Changes / Removal

- Changes made to a network account (i.e. network access, email) must be submitted by the Department Head.
- Password resets must be requested by the network user of that account or their Supervisor/Department Head. Steps will be taken to verify the identity of the user.
- A locked account must be requested to be unlocked by that account's user or their Supervisor/Department Head.
- All County User Accounts will be disabled if that user leaves their department. A deletion date will be entered into the disabled account 90 days from the disabled date.
- All network accounts that reach their deletion date will be deleted.
- Accounts used by staff on long term absence will be disabled, unless specified by the Department Head.

The following activities are prohibited at St. Lawrence County (not limited to these):

Security-Specific Unacceptable Use

The following activities are deemed inappropriate uses of St. Lawrence County systems and services, and are strictly prohibited. Inappropriate use includes, but is not limited to:

- Users are not authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing county-owned resources
- Introducing malicious programs into the network or a system (e.g., viruses, worms, Trojan horses, keystroke loggers, etc.)
- Effecting security breaches or disruptions of network communication

- Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a system or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Port scanning or security scanning is expressly prohibited unless prior authorization is granted
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
- Circumventing user authentication or security of any host, network or account
- Introducing honeypots, honeynets, or similar technology on the corporate network
- No servers (i.e. running web or FTP services from user workstations) or devices that actively listen for network traffic are allowed to be put on the corporate network without prior authorization by the IT Department
- Interfering with or denying service to any user (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet
- Users shall not send employee-related or county-related sensitive information that is not appropriately protected.
- Users shall not open message attachments or click on hyperlinks sent from unknown or unsigned sources. Attachments/links are the primary source of malware and social engineering and should be treated with utmost caution.

For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the help desk or IT administrator to obtain a password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to Internet services.

Messaging Sensitive Information

St. Lawrence County policies regarding sensitive data and disclosure should be observed when electronic communications are used. All reasonable precautions should be used to protect the integrity and confidentiality of this information.

- Users shall not transmit protected information via the county's default email system as it does not encrypt the information.

- There shall be no programming in place that automatically forwards all of a user's e-mail messages to an external e-mail address or other messaging system
- Users shall take extra precautions when transmitting Company Private/Sensitive information, government- sensitive or customer-sensitive information, including PII, via electronic messaging. Sensitive material should be marked and encrypted appropriately.
- Users shall take precautions to safeguard local e-mail files, including archives and other .pst files, as well as any other messaging files

Clean Desk Rules

Utilizing best practice to set goals to ensure that all sensitive materials, such as information about an employee, a customer, or intellectual property, are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. This will help reduce the risk of security breaches in the workplace and is part of standard basic privacy controls.

- Employees are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period
- Computer workstations must be locked when workspace is unoccupied
- Computer workstations must be shut completely down at the end of the work day unless instructed otherwise by IT
- Keys/badges used for access to restricted or sensitive information must not be left at an unattended desk
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location
- Whiteboards containing restricted and/or sensitive information should be erased or appropriately secured.
- Secure portable computing devices such as laptops and tablets

Removable Media Use

Removable media is any type of storage device that can be removed from a computer while the system is running and is a known source of malware infections and loss or theft of sensitive data for organizations. Examples include flash/thumb drives, memory cards, CDs/DVDs, external hard drives, or mobile devices used for storage purposes such as MP3 players or Smartphones. Use of such media must be controlled when conducting business operations.

- Removable media is permitted only if such media is county-issued and authorized. The IT Department must authorize the use of any personal or third-party owned/issued removable media for business use or for connecting to the Company network
- Information should only be stored on removable media when required in the performance of the user's assigned duties
- Upon completion of the assigned duties, all data shall be deleted from the removable media

- Use of removable media is not allowed on external or non-county-issued systems
- All removable media must be turned into the IT HelpDesk for proper disposal when no longer required for business use
- Any unknown removable media that is found unattended, must be reported to the IT Department and NOT attached to any IT Resource
- Use of removable media to introduce malware or other unauthorized software into the Company environment is strictly prohibited

Email Acceptable Use

1. Email access at St. Lawrence County is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account and password information.

2. Email access will be terminated when the employee or third party terminates their association with St. Lawrence County, unless other arrangements are made. St. Lawrence County is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased.

3. Email users will not auto-forward emails to accounts outside the control of St. Lawrence County.

4. Individuals at St. Lawrence County are encouraged to use email to further the goals and objectives of St. Lawrence County. The types of activities that are encouraged include:
   - Communicating with fellow employees, business partners of St. Lawrence County, and clients within the context of an individual's assigned responsibilities.
   - Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
   - Participating in educational or professional development activities.

5. St. Lawrence County's email systems and services are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared drive). Individual email use will not interfere with others' productive use of St. Lawrence County's email system and services.

6. Email use at St. Lawrence County will comply with all applicable laws, all St. Lawrence County policies, and all St. Lawrence County contracts. Use in a manner that is not consistent with the mission of St. Lawrence County, misrepresents St. Lawrence County or violates any St. Lawrence County policy is prohibited.

7. The following activities are deemed inappropriate uses of St. Lawrence County email systems and services, and are strictly prohibited. Inappropriate use includes, but is not limited to:
   - Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation,

forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

- Use of email in any way that violates St. Lawrence County's policies, rules, or legislative orders.
- Viewing, copying, altering, or deletion of email accounts or files belonging to St. Lawrence County or another individual without authorized permission.
- Sending of unreasonably large email attachments. The total size of an individual email message sent (including attachment) should be 25 MB or less. Users with a need to send larger attachments should contact the IT Dept. for alternative options such as use of an FTP resource.
- Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing email account passwords with another person, or attempting to obtain another person's email account password. Email accounts are only to be used by the registered user.
- St. Lawrence County prohibits use of its email systems and services for unsolicited mass mailings, non-St. Lawrence County commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

8. The email systems and services used by St. Lawrence County are owned by the county, and are therefore its property. This gives St. Lawrence County the right to monitor any and all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the legal team during the email discovery phase of litigation, observation by management in cases of suspected abuse, or to monitor employee efficiency.

9. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with St. Lawrence County's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence.
    - Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access by county delegates for a variety of management and legal needs. Both backups and archives are governed by the county's document retention policies.

10. If St. Lawrence County discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, email records may be retrieved and used to document the activity in accordance with due process.

11. Use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all email messages sent outside of St. Lawrence County become the property of the receiver.
12. Any allegations of misuse should be promptly reported to the IT Helpdesk. If you receive an offensive email, do not forward, delete, or reply to the message. Instead, report it directly to the IT Helpdesk.

13. St. Lawrence County assumes no liability for direct and/or indirect damages arising from the user's use of St. Lawrence County's email system and services. Users are solely responsible for the content they disseminate. St. Lawrence County is not responsible for any third-party claim, demand, or damage arising out of use the St. Lawrence County's email systems or services.

Internet Acceptable Use

1. Internet access at St. Lawrence County is controlled through individual accounts and passwords. Department managers are responsible for defining appropriate Internet access levels for the people in their department and conveying that information to the IT Department.

2. Each user of the St. Lawrence County system is required to read this Internet policy and sign an Internet use agreement prior to receiving an Internet access account and password.

3. St. Lawrence County may monitor any Internet activity occurring on St. Lawrence County equipment or accounts. St. Lawrence County currently employs filtering software to limit access to sites on the Internet. If St. Lawrence County discovers activities that do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

4. Individuals at St. Lawrence County are encouraged to use the Internet to further the goals and objectives of St. Lawrence County. The types of activities that are encouraged include:
   - Communicating with fellow employees, business partners of St. Lawrence County, and clients within the context of an individual's assigned responsibilities
   - Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities
   - Participating in educational or professional development activities

Unacceptable Use

1. Individual Internet use will not interfere with others' productive use of Internet resources. Users will not violate the network policies of any network accessed through their account. Internet use at St. Lawrence County will comply with all Federal, State, and Local laws, all St. Lawrence County policies, and all St. Lawrence County contracts. This includes, but is not limited to, the following:
   - The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).

- The Internet may not be used in any way that violates St. Lawrence County's policies, rules, or legislative orders including, but not limited to, [Social Media Policy, Email and Messaging Acceptable Use Policy, any applicable code of conduct policies, etc.]. Use of the Internet in a manner that is not consistent with the mission of St. Lawrence County, misrepresents St. Lawrence County, or violates any St. Lawrence County policy is prohibited.
- Individuals should limit their personal use of the Internet. St. Lawrence County allows limited personal use during breaks or lunch periods as long as it does not interfere with County Business or use excessive network resources. Personal use is subject to department rules, and management discretion.
- St. Lawrence County prohibits use for mass unsolicited mailings, access for non-employees to St. Lawrence County resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, commercial activity, and the dissemination of chain letters.
- Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by the Information Technology Department.
- Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to St. Lawrence County or another individual without authorized permission.
- In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business purposes.
- Employees of St. Lawrence County will treat all other individuals, clients, employees, etc. they interact with in any virtual, online forum or network capacity, in accordance with applicable county policies and basic corporate social decorum.

Information AUP

1. The primary responsibility for recommending changes to the AUP belongs to the IT Director for St. Lawrence County with input from the County Administrator, HR Director, and County Attorney.

2. The IT Director is responsible for ensuring any of St. Lawrence County's technical systems can meet our risk management needs as defined by best practices and compliance rules. All projects that use or require access to information handling systems (email, file shares, website, ERP, etc.) must be introduced through the IT department.

3. St. Lawrence County's Human Resources Director is responsible for ensuring St. Lawrence County rules and policy on acceptable use of equipment are explained clearly as part of St. Lawrence County's orientation training for new staff.

4. All St. Lawrence County staff, (including temporary staff such as interns), who have access to and make use of IT equipment and St. Lawrence County IT systems are responsible for using it in accordance with the rules within this policy. In particular, all staff must ensure that they use systems in such a way that they ensure client and staff confidentiality is maintained.

5. The effectiveness of this policy will be ensured by way of an on-going review of reports and logs available to the IT Department as part of the Information Technology Department's security procedures. It is expected that IT service desk will record any incidents showing non-compliance. A database is maintained by the IT service desk to allow for review of any patterns.
    - New members of staff are given a copy of the AUP as part of employee orientation.
    - St. Lawrence County's Department Heads may also be asked to confirm that this policy is effective within the departments they oversee. Results of audits of local IT systems will be reviewed to ensure that a picture is obtained of the extent to which the Acceptable Use Policy is clearly understood by all staff.
    - Local experts and departments are expected to audit their own practices from time to time to measure compliance with this policy or in light of future St. Lawrence County requirements.

6. Staff will only access IT systems provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.
    - Any changes to information access designed to expand use or change the storage location of information sources requires approval through IT's Access Authorization Form.

7. St. Lawrence County systems must not be used for the creation, transmission, or deliberate reception of any images, data, or other material that is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, staff are expected to conduct themselves in an honest, courteous, and professional manner.

8. St. Lawrence County systems must not be used for private work, or for storage of personal non-work related files.

9. Staff may not use St. Lawrence County's IT facilities for commercial activities. This includes, but is not limited to, advertising or running any sort of private business.
    - Use of the internet facility for commercial activities other than in the conduct of St. Lawrence County business is prohibited.
    - Use of the internet facility for political activities is prohibited.
    - Staff may not use St. Lawrence County's IT facilities for advertising or fundraising for commercial or charitable organizations not directly connected with St. Lawrence County.

10. It is the responsibility of all staff to ensure that computer systems and facilities and the data, which is accessed through them, are safe and secure. Systems should be placed in an area where it is not likely to be damaged and where the content of screens cannot be read by unauthorized people.

- Any member of staff who suspects or is made aware of a security breach must immediately alert the IT Helpdesk who will initiate investigation procedures. Depending on the breach scenario, investigations will be carried out jointly with St. Lawrence County's IT Management and appropriate senior management. If warranted, the findings will be subsequently reported to St. Lawrence County Board of Legislators.

11. Deliberate activities with any of the following consequences (or potential consequences) are prohibited:
    - Corrupting or destroying other users' data.
    - Using systems in a way that denies service to others (e.g. overloading the network).
    - Wasting staff effort or computing resources including staff involved in the support of those resources.
    - Gaining access to systems that you are not authorized to use.

12. The County email system should not be used for personal email. The County does recognize that critical notifications from schools and families are important, and that these communications are allowed on a limited basis.

13. No personally identifiable information or records should be transmitted via email to any external account, including personal accounts of St. Lawrence County employees. End users are not to provide records to co-workers who do not have access to the system or are outside of the county.

14. Staff should treat email attachments that have been sent unsolicited with extreme caution, especially if the sender is unknown. Viruses are often sent this way. If staff are not sure what an attachment is for, or why someone has sent it to them, they should not open it, and seek advice from the IT Helpdesk.

15. When sending emails to a distribution list:
    - Do not send or forward email to any large group of staff unless there is a genuine reason for them to read it.
    - Do not circulate warnings about any virus risk, but consult with the IT Helpdesk.
    - When sending email to external addresses, consider the possibility that this action may inadvertently reveal email addresses to third parties.

16. Forging an email (or any other electronic message), or sending email from any account other than your own without permission is not permitted.
17. Email will not be used for intentional receipt and/or distribution of offensive, obscene, or pornographic material. There is a legal requirement to report any computer crime involving child pornography to law enforcement. If staff receive an email connected with child pornography, they should seek advice from their supervisor immediately so that St. Lawrence County can take appropriate preventative action.
    - If staff receive any pornographic or offensive email, they should not open it or print it. Staff should contact the IT Helpdesk to report it.

- If staff receive an email containing sexually or racially abusive or discriminatory phrases or material, again they should seek advice from their supervisor.
- No member of staff is permitted to distribute email that contains offensive material. Offensive material is defined by St. Lawrence County's Equal Opportunity and Harassment Policies and includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive. Other than instances which demand criminal prosecution, St. Lawrence County is the final arbiter on what is or is not offensive material, or what is or is not permissible use of email.

18. Any computing system owned or provided by St. Lawrence County is subject to the same conditions of use whether used at home or in the office. Users should take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work

19. The use of any customer/client identifiable information on staff-owned equipment is strictly forbidden without the authorization of the Department Head.
    - St. Lawrence County business information (such as spreadsheets, plans, and reports etc.) may be used, but not be stored permanently on staff-owned equipment or user-acquired applications.
    - To restrict the possibility of viruses being transmitted to the organizational computers and network, staff must not use their own computer for work-related activities unless anti-virus software and a firewall have been installed and are regularly updated.
    - Personal mobile devices may be synchronized with work email for calendar, contact, and email purposes where permitted by email policies and guidance.
    - In circumstances where the organizational resources do not meet the needs of end users, project or access requests can be submitted through normal IT channels.

20. On request, using the Access Authorization Form, the IT department will provide each member of staff with a personal username/password. These must be used to gain access to any St. Lawrence County computer. Usernames/passwords will only be issued when authorized by an appropriate authorized signatory, and when identity checks have been completed satisfactorily.
    - Before a password is issued, staff must complete the appropriate authorization forms that will request the user to read, understand, and abide by the terms of this overarching Acceptable Use Policy.

21. The IT department will endeavor to provide all systems with secure access facilities. Access to databases or systems containing important, sensitive, and/or confidential information will be restricted to those staff who require access as part of their job function. These may be protected by additional security controls.
    - Where passwords are used, users will be able to select and change their own password by using a minimum of 12 characters (numbers, letters, and special symbols).
    - Users should not leave any computer unattended without either logging out or activating a password-protected screensaver. Where a previous user has left their access open, new users must log out from that session first.

- Users should not add additional password or security measures to any computer or mobile device or files without first consulting with the IT department.
- Attempting to remove or bypass any security access on any St. Lawrence County computers is strictly forbidden.
- Passwords are issued for personal use only. They should not be shared or disclosed to anyone else. Users are required to protect their usage against loss, damage, or theft and against possible misuse by others. If a breach of security is recorded, the burden of proof will be with the registered user to show that they are not responsible for the breach.
- Users should report any known or suspected breaches of information security to the IT Helpdesk for any necessary action to be considered and undertaken.

22. All staff are responsible for ensuring that confidential information is stored securely and that appropriate confidentiality is maintained when handling information.

High Risk Information

- Confidential St. Lawrence County information should only be stored within a shared folder on the St. Lawrence County network, within a user's "My Documents" folder, or to a St. Lawrence County supplied encrypted laptop or memory stick. At no time should data be stored in any other location. Individual users' "My Documents" folders are held in a secure location on the St. Lawrence County network.

23. Access to read the document archives will only be granted to staff responsible for investigating system failure or system misuse, and then only to look at information as necessary to repair or protect the systems or to investigate use that may be in contravention of this AUP.
    - Document files, web browsing logs, email or voicemail messages, however confidential or damaging, may have to be disclosed in court proceedings or during internal investigations if relevant to the issues being investigated.
    - Access to a user's personal documents, either stored or held in an email mailbox, will only be granted to another user if a written request with appropriate reasons is received from the appropriate Department Head, County Attorney, or County Administrator.

24. The IT department schedules fileserver backups to enable recovery from any system failure.
    - It is essential that staff save their work to a network share provided by IT, not to their local hard drive.
    - Accounts not used for [3 months] (without prior warning) may be deleted under the assumption that the employee has left the organization.
    - If users change job role, they should ensure computer access has been amended appropriately using an Access Authorization Form
    - If users change their job role, they should hand-over all relevant personal files and email messages to their manager.

25. When informed by the HR department that a member of staff has ceased employment, the IT department will oversee the deletion or transferal of all information pertaining to that user.
    - Staff who cease employment with St. Lawrence County, should take responsibility to hand over all appropriate personal computer files and email messages, either by forwarding them to a line manager, by copying them to a shared area, or by simply deleting them.

26. Remote control software is used by the IT department to connect and take control of a computer remotely. IT staff will not use this to connect to a computer without attempting to contact the user of the machine first. Access to this software is only permitted by IT staff.
    - Remote access will not be given for other purposes, such as allowing managers to monitor their staff's work.
    - Staff should not attempt to use any remote control software, nor allow external users or support staff to use it without the express permission of the IT department.

27. Access to the Internet is primarily provided for work-related purposes. Reasonable personal use is permitted provided this does not interfere with the performance of duties or adversely affect system performance. St. Lawrence County has the final decision on what constitutes excessive use. Staff may access some services (e.g. personal email or online banking) provided these are within the boundaries of incidental personal and acceptable use. St. Lawrence County cannot guarantee the privacy of staff accessing these facilities from work.
    - Personal access to the Internet can be limited or denied by a supervisor. Staff must act in accordance with their department guidelines.
    - The IT department has the right to withdraw internet access from any user and globally ban access to any site as appropriate, without warning.
    - Unless specifically authorized, no member of staff may post messages under St. Lawrence County's name to any newsgroup or chat room.
    - Unless specifically authorized by the IT department, no member of staff may publish a website under the name of St. Lawrence County or featuring its logo.
    - St. Lawrence County will not accept liability for personal legal action resulting from staff misuse of the Internet.
    - Access to file downloads will be restricted as necessary by IT to ensure system security.
    - St. Lawrence County reserves the right to monitor all internet accesses, including but not limited to email and web access. No member of staff should consider information sent/received through the Internet as his/her private information.
    - No member of staff may access, display, or download from internet sites that hold offensive material.
    - Personal/employee identifiable data must not be published in any way on the Internet without the express consent of each and every individual concerned.

28. All software must be purchased, installed, and configured by the IT department, or with the IT department's knowledge and approval; this includes all software packages,

software upgrades, and add-ons, however minor. It also includes shareware, freeware, and any items downloaded from the Internet. Under no circumstances should any software be purchased or installed without the explicit agreement of the IT department.

- Do not violate the license agreement by making illegal copies of St. Lawrence County software. Anyone found doing so may be prosecuted under applicable local, state, and federal law.
- Software not licensed to St. Lawrence County must not be loaded onto St. Lawrence County computers. Software licensing will be arranged and recorded by the IT department as part of the procurement and /or installation process.
- Users are not allowed to download software from the Internet or install from CD or disc without IT department authorization. Any unlicensed software found on a St. Lawrence County computer will be automatically deleted or disabled, and disciplinary action may be taken.

29. The use of any software package to access, modify, or analyze St. Lawrence County's data for either work or personal purposes is forbidden without prior approval. The expectation is that this use constitutes a short-term pilot.
    - There should be no expectation that long-term use will be permitted or that St. Lawrence County will pay for personal software. Any information created or used must be stored appropriately based on the storage and retention rules that govern that information source.

Mobile Device Management

1. It is the responsibility of any employee of St. Lawrence County who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct St. Lawrence County business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the county's systems, data, users, and clients at risk.

2. All personal mobile devices may be allowed to access county email and related calendar, task, and contact information ONLY. These mobile devices should be secured with password or PIN.

Security

1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password or a PIN. All data stored on the device should be encrypted using strong encryption. Employees agree to never disclose their passwords to anyone, even to family members, if business work is conducted from home.

2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data.

3. Any non-county computers used to synchronize or back up data on mobile devices will have installed up-to-date anti-virus and anti-malware.

4. Passwords and other confidential data, as defined by St. Lawrence County's IT department, are not to be stored unencrypted on mobile devices.

5. Any mobile device that is being used to store St. Lawrence County data must adhere to the authentication requirements of St. Lawrence County's IT department.

6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with St. Lawrence County's overarching security policy.

7. Employees, contractors, and temporary staff will follow all county-sanctioned data removal procedures to permanently erase county-specific data from such devices once its use is no longer required.

8. In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to IT immediately. The device will be remotely wiped (if possible) of county data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

Hardware & Support

1. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the county network.

2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jailbreaking, rooting) without the express approval of St. Lawrence County's IT department.

3. IT will support the connection of mobile devices to county resources. On personally owned devices, IT will not support hardware issues or non-county applications.

Social Media Usage

1. St. Lawrence County's social media accounts are intended to be used solely for business purposes.

The following are examples of legitimate business usage of public social media:

- Building positive brand image.
- Increasing mind share: Social media can reach large audiences at very low monetary cost, giving St. Lawrence County another medium for promotion, increasing visibility and outreach.
- Providing citizens with more timely and personal service in the medium that they prefer will increase satisfaction.
- Monitoring public opinion on St. Lawrence County and its products and services.
- Professional networking, such as maintaining academic contacts or maintaining contacts with members of professional or standards organizations.
- Quickly and efficiently responding to customer service issues. The answer to a problem can be public, making it searchable by other customers that have the same request.

The following activities are deemed inappropriate uses of social media:

- Use of social media for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of social media that in any way violates St. Lawrence County's policies, rules, or administrative orders.
- Opening attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing social media account passwords with another person, or attempting to obtain another person's social media account password.

2. Use of personal social media accounts and user IDs for county use is prohibited.

3. Use of St. Lawrence County social media user IDs for personal use is prohibited. Examples of prohibited use of St. Lawrence County User IDs include: downloading and installing plug-ins or helper applications such as those that try to access the county email directory, joining groups using a St. Lawrence County

user ID for personal reasons, or adding personal friends to an employee's friends list.

Telephone and voicemail

As with all St. Lawrence County resources, the use of telephones and voicemail should be as cost effective as possible and in keeping with the best interests of St. Lawrence County. All employees must operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of St. Lawrence County.
- The IT Department is responsible for installation and repair of all St. Lawrence County telephony equipment and administration of telephone and voicemail accounts. Call the IT Helpdesk to report any troubles or request any changes.
- Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring the IT Department is notified of any adds, moves, or changes required to telephone or voicemail services.
- All new county employees with a regular office space will be issued a telephone. Each has a direct line and an extension. Each also has a voicemail box which must be configured upon first use.
- All voicemail boxes will be protected with a PIN (personal identification number) which you will select. PINs must not be shared with others. You should personalize your PIN and voicemail box during the initial configuration.
- A voicemail box can hold a limited amount of message storage time. If a voicemail box is full, no further messages can be recorded. Voicemail should be checked and cleared out on a regular basis.
- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.
- Dial "8" for an outside line.
- Dial "911" directly to report an emergency, just as you would on a regular phone.

Unacceptable Use

St. Lawrence County telephone and voicemail services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.
- Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.
- Using the telephone system or breaking into a voicemail box via unauthorized use of a PIN or other password.
- Broadcasting unsolicited personal views on social, political, or other non-business related matters.
- Soliciting to buy or sell goods or services unrelated to St. Lawrence County.
- Calling 1-900 phone numbers.

- Making personal long-distance phone calls without supervisor permission.

Misuse of telephone and voicemail services can result in disciplinary action, up to and including termination.

Monitoring

St. Lawrence County reserves the right to monitor telephone and voicemail use, including telephone logs and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

Service and Repair

The IT Department requests three days' notice to set up a standard telephone service and voicemail box.

If there is a problem with an existing telephone or voicemail box, contact the IT Helpdesk immediately at 2323 or Helpdesk@stlawco.org.

Removable Media

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the county's systems, data, users, and clients at risk.

Security

2. All USB-based devices that are used for business interests must be pre-approved by IT, and must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed whatever anti-virus and anti-malware software is deemed necessary by St. Lawrence County's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be used must be updated in accordance with existing company policy.

3. All removable media will be subject to quarantine upon return to the office before they can be fully utilized on enterprise infrastructure.

4. Passwords and other confidential data as defined by St. Lawrence County's IT department are not to be stored on portable storage devices.

5. Any USB-based memory device that is being used to store St. Lawrence County data must adhere to the authentication requirements of St. Lawrence County's IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by St. Lawrence County's IT department before any enterprise data-carrying memory can be connected to it.

6. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. See the IT Policy folder for detailed data wipe procedures for flash memory.

Help & Support

7. St. Lawrence County's IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media. This applies even to devices already known to the IT department.

8. Employees, contractors, and temporary staff will make no modifications of any kind to county-owned and installed hardware or software without the express approval of St. Lawrence County's IT department. This includes, but is not limited to, reconfiguration of USB ports.

9. IT may restrict the use of Universal Plug and Play on any client PCs that it deems to be particularly sensitive. IT also reserves the right to disable this feature on PCs used by employees in specific roles.

10. IT reserves the right to summarily ban the use of these devices at any time. IT need not provide a reason for doing so, as protection of confidential data is the highest and only priority.
11. IT reserves the right to physically disable USB ports to limit physical and virtual access.

12. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

Organizational Protocol

13. IT can and will establish audit trails in all situations it feels merited. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to St. Lawrence County's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains St. Lawrence County's highest priority.

14. The end user agrees to immediately report to his/her manager and St. Lawrence County's IT Department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

15. Any questions relating to this policy should be directed to the IT Helpdesk at 2323.

Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at St. Lawrence County. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Suspension of network use and rights.
- Disciplinary action according to applicable St. Lawrence County policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Approval

This policy was approved by the St. Lawrence County Board of Legislators at its December 2, 2019 regular meeting.

Agreement

I have read and understand the St. Lawrence County Information Technology Acceptable Use Policy. I understand that if I violate the rules explained herein, I may face disciplinary or possible legal action as outlined in this acceptable use policy.

_____
Employee Name

_____ _____
Employee Signature Date

Revision History

Version	Change	Author	Date of Change