(IS) Technology Acceptable Use Standards

Effective Date: January 2020

Owner	Information Services (IS) Director, IS Division Directors
Reviewer(s)	IS Division Directors and IS Technology Services Managers
Approver(s)	IS Director and IS Division Directors
Related Policies	(IS) Information Technology Policy Adopted 1/20 Conduct and Performance Policy (BOC Only) Adopted 11/89; Revised 6/92, 12/96, 4/06, 10/15, 1/20 No Harassment and No Discrimination Policy (BOC Only) Adopted 6/92; Revised 4/00, 4/06, 12/11
Related Standards	(IS) Technology User Account Standards (IS) Technology Infrastructure Security Standards (IS) Network Security Standards
Storage Location	iCobb
IS Last Review Date	December 2019
IS Next Review Date	December 2021
IS Review Cycle	Every two years
Employee Acknowledgement	Annually

1. PURPOSE

To outline appropriate and inappropriate use of Cobb County Government (County) Technology Resources to minimize disruptions to services and activities, as well as comply with applicable policies and laws. The Information Services Department (IS) is responsible for the management of County technology resources. These resources include, but are not limited to: Internet access, intranet, email systems, instant messaging, collaboration tools (Skype/Teams, Planner), desktop and mobile devices, storage media, hardware, software uploads/downloads, file transfer protocol (FTP), and applications.

Pursuant to the Information Technology Policy, the IS Director is authorized to create, maintain, and communicate information technology and security standards concerning the use, protection, and preservation of County information systems and technology resources.

2. SCOPE

These standards apply to all County agencies, elected offices, Departments, full-time, part-time and non-employees (temporary employees, volunteers, service providers, vendors, contractors, and any other entities) that access County technology resources. If you have questions regarding these standards, contact the IS Technical Operations Division Director at 770-528-8740.

3. GOVERNING LAWS, REGULATIONS & STANDARDS

Guidance	Section
Georgia Computer Systems Protection Act	O.C.G.A. 16-9-90, et seq.
Georgia Open Records Act	O.C.G.A. 50-18-70, et seq.
Georgia Archives as adopted by County Code	https://www.georgiaarchives.org/records/retention_schedules
And all other applicable laws and regulations	

4. DEFINITIONS

Encryption - A process that transforms readable data into a form that appears random and unreadable to unauthorized users.

File Transfer Protocol (FTP) - a communications protocol that is used to connect two computers over the Internet so that the user of one computer can transfer files and perform file commands on the other computer. Companies will often create FTP sites to allow sharing of large files.

Mobile Device - a wireless, portable device that allows you to access data and information from the County's internal network.

Personal Device - Any device not owned by Cobb County (including but not limited to laptops, desktops, smartphones, cellular phones and tablets).

Privileged or Confidential Information - Employees who deal with plans, programs, and other information of significant interest may only release information that they have authority and responsibility to release to persons authorized to receive such information.

Agency/Department Heads, Division Managers, other supervisors, and Department representatives who are entrusted with confidential employee information must hold that information in the strictest confidence. Unless the information needs to be conveyed for a business purpose, the information should not be discussed or shared with other employees

Public Information - Public information requires minimal protection. The risk to the government or our customers is negligible if this information is disclosed or modified. This includes information that is required to be public information by law.

Restricted Information - Restricted information is extremely sensitive. Information in this classification must have one or more of the following attributes:

- Outside disclosure is prohibited.
- Outside disclosure would compromise the County's data and network security infrastructure.

Third-Party - Any Non-County individual or organization that develops, installs, delivers, manages, monitors, or supports any Local Agency IT Resource

5. STANDARDS

The County provides technology resources to allow you to work easily and efficiently. When using these resources, you must be mindful of our standards to protect the County and our assets from security threats, such as malware attacks, viruses or other network security vulnerabilities, and from possible lawsuits and fines. These standards apply to anyone who uses or accesses County technology resources, and you have a responsibility to know and follow them.

5.1. Access to County Technology Resources

5.1.1 When you access County technology resources, you must do so responsibly while also protecting those resources from viruses, theft or misuse.

5.1.2 Access is controlled through individual accounts and passwords. Access must be approved by your manager/supervisor. It is your responsibility to protect the confidentiality of your account and password information.

5.1.3 The technology resources used at or on behalf of the County are owned by the County, and are therefore its property. This gives the County the right to monitor any and all traffic passing through its systems. Except for confidentialities created by law (such as Attorney-client

communications), **you should not have any expectation of privacy while using the County's technology resources.**

5.1.4 The level of access to information systems, websites, and applications via the Internet is Department specific and based on the business requirements of the Department. The Department Management will notify IS of required access levels. If the Department is maintaining application access, it must keep a record of the level of access provided to the user. IS will implement controls to enforce Department policy. This excludes access to malicious or inappropriate websites that will be controlled by IS.

5.1.5 Computer files and electronic communications via the Internet, intranet, collaboration tools, or email are subject to the Georgia Open Records Act. This includes information on personal devices if you use them to access County controlled information.

5.1.6 You should not transmit restricted information over the Internet unless it is secure/encrypted. IS provides a secure data transfer method; see section 5.6 "File Transmissions" below for details. Contact the IS Call Center at 770-528-8740 for additional information.

5.1.7 You should not attach any wireless access point to the County network. All access points between County networks and the Internet shall be managed by IS. In special cases written authorization for exceptions to these standards may be granted as agreed upon by the IS Director (see section 6 "Exceptions" for details).

5.1.8 You should not install any software products on County owned devices without approval from the County's IS Department. Contact the Call Center at 770-528-8740 for approval instructions.

5.1.9 You should notify IS immediately if you lose a County device or personal device containing County information or if the device is stolen. IS will then immediately unregister the device from all access points.

5.2. Email

5.2.1 Email Account Creation

5.2.1.1 All County employees will receive an email account. Temporary email accounts will be granted to third-party non-employees on a case-by-case basis. Possible non-employees who may be eligible include:

1. Contractors
2. Vendors
3. Interns
4. County Board and Committee members

(IS) New Employee Access Request: Go to iCobb > Forms to complete request for email access.

5.2.2 Email Retention

5.2.2.1 Pursuant to the Information Technology Policy, the County retention period for email in the Outlook system is 5 years. Departments, agencies and employees are responsible for the retention of emails or records in compliance with all applicable laws and regulations, including the Local Government Record Retention Schedules. Email older than 5 years will be automatically deleted. There are two exceptions to the 5-year retention policy: 1) County Policy makers (e.g., Commissioners, Agency Directors, Department Directors, Attorneys, Police Department Command Staff, etc.) and 2) Items placed in the "Retention >5 Years" folder.

5.2.2.1.1 County Policy Makers
IS will not subject County Policy Makers to the 5-year retention period. All Agency Directors, Department Directors, County Manager, and Elected Officials are policy makers. If you are a policy maker and not included in this list, you must notify IS to retain your email beyond 5 years.

5.2.2.1.2 Retention > 5 Years Folder
IS will create a folder in every Outlook mailbox called “Retention > 5 Years”. You are responsible for moving emails and attachments to this folder if you are required by law or policy to keep the contents more than 5 years.

5.2.2.1.2.1 You, your management, and IS each have a responsibility to ensure the contents of your “Retention > 5 Years” folder is saved or moved when you leave your Department. IS will coordinate with Department managers for disposition of emails in the “Retention >5 Years” folder for all persons listed on the HR termination list and for all employee transfer forms.

5.2.2.2 Email stored on your local computer in a pst file format is not backed up unless you store a copy on a network drive.

5.2.2.3 Archival and backup copies of email messages may exist, even if you delete them from your email box.

5.2.2.4 To the extent required by law, including, but not limited to the Georgia Open Records Act, O.C.G.A. § 50-18-90 et seq., each individual County department and agency shall be responsible for complying with all applicable laws and regulations, including the Local Government Record Retention Schedules.

5.2.3 Email Account Termination

5.2.3.1 When you leave the County, your mailbox will be retained for 90 days prior to deleting, unless otherwise requested by the Agency/Department Head.

5.2.3.2 If you have content in your “Retention >5 Years” folder you are required to notify IS when you retire or leave the County.

5.2.3.3 You, your management, and IS each have a responsibility to ensure the contents of your “Retention > 5 Years” folder is saved or moved when you leave the County. IS will coordinate with Department managers for disposition of these emails for all persons listed on the HR termination list.

(IS) Disable Employee Active Directory Account Request: Go to iCobb > Forms to request email account termination.

5.2.4 Email Use

5.2.4.1 Use caution when communicating via email. Keep in mind that all email messages sent outside of the County become the property of the receiver. Consider not communicating anything that you wouldn’t feel comfortable being made public. You should demonstrate care when using the “Reply All” command during email correspondence to ensure the resulting message is not delivered to unintended recipients.

5.2.4.2 Suspicious emails may contain malicious attachments or harmful links. You should use the County supplied reporting tool, which communicates with the IS security team to flag suspicious or malicious emails.

5.2.4.3 You should promptly report any allegations of misuse of email to your manager/supervisor. If you receive an offensive email, do not forward, delete, or reply to the message, but report it to your manager/supervisor. Managers and Supervisors should determine the appropriate course of action and may contact IS (770-528-8740), the County Attorney's office (770-528-4000) or HR (770-528-2541) for assistance if needed.

5.2.5 Email Archiving

5.2.5.1 Pursuant to the Information Technology Policy, the County archives all incoming and outgoing email onto a separate storage system. Archived emails will be retained for 10 years unless on administrative or legal hold. Email older than 10 years will be purged. Prior to initiating the first 10-year purge (2030), IS will seek approval from the County Attorney. The email archival system is the official system of record for email open records requests.

5.3. Connectivity to County Network

5.3.1 Direct Connect

There are two methods by which you can directly connect to the County network:

1. Wired Network Connection
2. Wi-Fi

5.3.1.1 Wired Access

Offices and conference rooms in County buildings are equipped with hard-wired network access ports. These provide direct connectivity to the County network. These connection ports are to be used for official County business.

5.3.1.1.1 You must use equipment approved by IS to attach directly to a County network.

5.3.1.1.2 Connectivity of your personal devices via an access port requires advance approval of IS Technical Operations Division.

5.3.1.1.3 You are not allowed to connect devices which broadcast DNS on the County network.

5.3.1.2 Wireless Access (Wi-Fi)

5.3.1.2.1 You may not install access points or wireless clients on the County network without approval of IS. If approved, IS will perform the installation.

5.3.1.2.2 All wireless access must be authenticated via an Access Control server or a centralized Authentication server. IS will configure and monitor the Authentication Server.

5.3.1.2.3 If you install a device in a non-approved manner, the actions may result in disciplinary action in accordance with the County's Conduct and Performance Policy (BOC Only). Go to iCobb or click the link above to access the policy.

5.3.2 Remote Access

Remote access may be established by IS for you if approved by your Agency/Department Head. You should be mindful that remote access can allow intruders access to County resources if misused. You are a key component to safeguard our technology resources from unauthorized access.

5.3.2.1 Virtual Private Network (VPN)

You can access the County network remotely via VPN if approved by your management and the IS Director. Approved County employees and all authorized third parties (customers, vendors, etc.) may utilize the benefits of VPN.

5.3.2.1.1 If you use VPN to access the County network, you are responsible to ensure that unauthorized users are not allowed access to County internal networks.

5.3.2.1.2 You must use your Active Directory login-in credentials to login to VPN (i.e. the login used to access your computer or email account).

5.3.2.1.3 While connected to the County network via VPN, you must not use the same computer to connect to another private network at the same time.

For example:

1. If you are a Cobb County employee and work part-time as a billing specialist for another business, you cannot login to Cobb County and your other employer's employee network at the same time from the same computer.

2. A Cobb County contractor/vendor cannot login on the County network and his/her employer's network or another client's network at the same time from the same computer.

5.3.2.1.4 By using VPN technology with personal equipment, you must understand that when connected, your devices are an extension of the County network. As such, they are subject to the same rules and regulations that apply to County-owned equipment while connected to the network. Your devices must be configured to comply with the County's policies and standards.

(IS) Employee VPN/Email Connectivity Request: Go to iCobb > Forms for more details.

5.3.3 Third-Party Access

The County has applications and hardware that are supported via third-party. The manager of the Department with which the third-party is doing business is responsible for approving access if needed. Offsite contractors and vendors must access County network connected hardware and/or software which the third-party vendor supports through the following steps:

1. Request and be provided an Active Directory account.
2. Establish a VPN remote access connection (permissions based on business support requirements).
3. Receive application specific access.

A third-party who has access to County network and technology resources is responsible for following the IT Policy and all related standards of the County. It is the responsibility of the sponsoring Agency/Department Head or designee to ensure the third-party is aware of the relevant IT Policy and related standards. These documents can be found on iCobb.

(IS) Vendor/Contractor VPN Connectivity Request: Go to iCobb > Forms for access details.

5.4 Personal Devices

5.4.1 Methods

Pursuant to the Information Technology Policy, you may utilize a personal device to access the County's technology resources if you have approval from your Agency/Department Head or designee and the IS Director. Although use of a personal device for County business purposes may be efficient, it is not the preferred method and may subject information on that device to Georgia's Open Records Act.

5.4.2 Risks

There are potential risks associated with accessing the County's network via your personal device. If you access the County's technology resources via your personal device, including but not limited to laptops, desktops, smartphones, cellular phones, and tablets, you should use the same security protocols as when using County equipment. Failure to do so could result in immediate suspension of all network access privileges, disciplinary action, termination of employment, and/or legal action according to applicable laws and policies. You should be aware that conducting County business and accessing County resources from your personal device may subject information on that device to Georgia's Open Records Act. Further, such use may be restricted by applicable laws and County policies.

5.4.3 Contact the IS call center at 770-528-8740 to determine if your personal device is compliant with the County's Standards. If a personal device is not compliant, it may not synchronize with the County's Outlook/Exchange System.

5.4.4 You must obtain written approval from your Agency/Department Head and the IS Director before attaching and synchronizing personal devices to the County's Outlook/Exchange System. The Department will be responsible for additional licensing.

5.4.5 Your device must be password protected.

5.4.6 Connection of your personal device may result in increased traffic or data cost dependent upon your individual plan. The County is not responsible for any of these charges.

5.4.7 IS Technical Operations or Client Services Divisions will assist with the setup of the device.

5.4.8 The Technical Operations and Client Services Divisions will provide assistance to the device owner for problem diagnosis and resolution when possible but is not responsible for the support, maintenance or operation of the device. IS will not be personally liable for any damages to the device as a result of troubleshooting activities.

5.5 Removable Media/USB Devices

You should **only** store sensitive information on your removable media/USB devices when it is absolutely necessary to minimize the risk of information loss and theft. You are responsible for protecting your removable media/USB from compromise.

5.5.1 IS reserves the right to refuse to connect removable media and USB devices to County and County-connected infrastructure. IS will refuse to establish a connection if the County's systems, data, users, or clients are at risk. Risks include possible infections by computer viruses or malware of County networking resources.

5.5.2 Users can contact IS to have removable media/USB devices scanned for viruses or malware prior to use. Contact the IS call center at 770-528-8740 for instructions.

5.5.3 Department Heads may request PCs in their area to have USB drives disabled. Contact the IS call center at 770-528-8740 for instructions.

5.6 File Transmissions

5.6.1 IS provides four methods of transferring files:

1. File Transfer Protocol (FTP) – a non-secure method available to you by request. FTP accounts are assigned to and should be used by an individual**,** not a Department and should not be shared. Please contact the Call Center at 770-528-8740 for instructions.

2. Citrix ShareFile – IS provides the capability to securely transfer files via Citrix, which can be obtained via a request from your manager/supervisor to IS. Your Department will be responsible for licensing costs for new ShareFile accounts. Please contact the Call Center at 770-528-8740 for instructions.

3. Email Attachments – IS authorizes email attachments up to 30 MB per file. This is the least secure method of file transfer.

4. Microsoft One Drive – County users who have Office 365 are permitted to use One Drive as a secure method to transfer files. Please contact the Call Center at 770-528-8740 for instructions.

5.6.2 Your manager or supervisor must notify IS when a user with a Citrix ShareFile or FTP account leaves his/her employment. If the Department is unsure, contact IS at 770-528-8740 for assistance.

5.7 Internet Websites

5.7.1 Pursuant to the (IS) Information Technology Policy, all County domain names must be approved by the IS Director and Communications Director. The domain name registration is controlled and maintained by the County Webmaster. Submit domain name requests to web@cobbcounty.org.

5.7.1.1 Elected Officials may obtain and maintain their own domain names. They should provide the domain name information to the IS webmaster at web@cobbcounty.org to ensure IS has a complete list of Cobb County domain names. IS does not maintain Elected Officials' domain security or websites.

5.7.2 Many viruses are found on unfamiliar or non-business-related websites. Examples of these sites include: gaming, pornography, and gossip sites. You must exercise extra caution when accessing unfamiliar websites to ensure you do not access an infected website.

5.8 Intranet Websites

5.8.1 In order to have information published on the County intranet, (iCobb), you must provide, at minimum, the following information to HR:

1. Contact name
2. Document retention information

5.9 Acceptable Uses

When you exercise the privilege of using the County's technology resources you agree to:

5.9.1 Use these technologies to conduct County business.

5.9.2 Ensure that your communications are professional, truthful, appropriate, and lawful.

5.9.3 Use language and subject matter that reflects business purposes and follows County policies, standards, and all state and federal laws.

5.9.4 Ensure that the activity does not interfere with your productivity.

5.9.5 Be responsible for the content of all communications you send over the Internet.

5.9.6 Be responsible and accountable for all computer transactions made with your user ID and password.

5.9.7 Verify and ensure the accuracy of any information obtained from Internet resources prior to using such information for a business purpose.

5.9.8 Check your email in a consistent and timely manner so that you are aware of important County announcements and updates, as well as for fulfilling business and role-oriented tasks.

5.9.9 Be responsible for managing your mailbox, which includes routine cleaning of email messages no longer required. If you subscribe to a mailing list, you must be aware of how to unsubscribe from the list and do so if no longer needed. There is a cost to the County associated with storing email messages.

5.9.10 Your Agency/Department Head will determine if you are authorized to use the Internet while using County equipment. Your Agency/Department Head may further restrict your Internet use, if acceptable use standards are not followed.

5.10. Prohibited Uses

Pursuant to the Information Technology Policy, when you exercise the privilege of using the County's technology resources you will not:

5.10.1 Create, send, copy, or forward any fraudulent, defamatory, obscene, threatening, intimidating, offensive, harassing, discriminatory, or disruptive messages, e-mails, or chain messages. Such prohibited uses include any communication which violates County policy, standards, and/or state or federal law. If a user receives material or suspect communications believed to be in violation of the County's No Harassment and No Discrimination Policy (BOC Only), **the user should report the incident** as advised in the No Harassment and No Discrimination Policy (BOC Only). (Go to iCobb > Policies to access the policy.)

5.10.2 Create, send, copy, or forward any messages, e-mails, or chain messages that violate the County's Conduct and Performance Policy (BOC Only).

5.10.3 Access, view or download any non-business-related information from any website, chat room, newsgroup, messaging, e-mail, or any other electronic location of an adult nature (obscene, sexual, or pornographic) unless pursuant to County business (i.e., law enforcement, public safety, sheriff, judicial).

5.10.4 Transmit any messages anonymously or using an assumed name; attempt to obscure the origin of a message; misrepresent your job title or position with the County; and/or allow any other person to utilize your protected information to access County resources or information.

EXCEPTION: The following groups are exempt:
- Law enforcement investigation units
- IS staff for cyber security training purposes

5.10.5 Engage in any illegal or unethical acts involving electronic communications, including criminal acts outlined in the Georgia Computer Systems Protection Act, O.C.G.A. Sec. 16-9-90, et seq. Criminal acts contained in that statute include: computer theft (unauthorized use with the intention to take, appropriate, obtain, or appropriate the property of another); computer trespass (unauthorized use with the intention of deleting a program or data, of interfering with the use of a program or data, or of altering, damaging, or causing a malfunction of a computer, computer network or computer program); computer invasion of privacy (use with the intention to examine employment, medical, salary, credit, or other financial or personal data without authority); computer forgery (creation, alteration, or deletion of data contained in any computer or computer network); and computer password disclosure (unauthorized disclosure of a password for accessing a computer/computer network).

5.10.6 Use another person's log-in credentials.

5.10.7 Access or download gambling sites.

5.10.8 Send information that violates or unlawfully infringes on the rights of any other person (including but not limited to copyrights and software licenses).

5.10.9 Download, install or run security programs or utilities such as password cracking programs, packet sniffer, or port scanners that reveal or exploit weaknesses in the security of technology resources.

EXCEPTION: The following groups are exempt:
- Law enforcement investigation units
- IS staff for cyber security training purposes

5.10.10 Engage in any unlawful or unreasonable use of technology not specifically addressed in the (IS) Information Technology Policy or these standards.

5.10.11 Circumvent County security measures.
Since it is impossible to specify every instance that might result in a violation of the (IS) Information Technology Policy and the Related Standards listed on the chart on page 1, a standard of reasonableness will apply to determine whether a user's use of technology is unacceptable.

5.11 Disclaimer of Responsibility

The County is not responsible for material that you view or download from the Internet. You are cautioned that, included among the massive amount of information on the Internet, some is offensive, sexually explicit, and inappropriate. In general, it is difficult to avoid coming into contact with some of this material on the Internet, even when performing innocuous search requests. In addition, having an Email address on the Internet may lead to receipt of unsolicited Email containing offensive content. When accessing the Internet, you do so at your own risk.

5.11.1 The County assumes no liability for any direct or indirect damages arising from your connection of personal equipment to the County's technology resources.

5.11.2 The County is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems.

5.11.3 You are solely responsible for any material that you access and disseminate through the Internet.

6. EXCEPTIONS

Exceptions to these standards must be justified and approved in advance. The County may deviate from the standards when:

1. Written justification is provided to the IS Director by the Agency/Department Director; and
2. A cost/benefit analysis has been performed by IS and the requesting Department showing:
   a) the available compliance options, and
   b) the risk of noncompliance; and
3. An acceptable balance between the costs and the risks has been determined to be acceptable to IS; and
4. The acceptance of risk has been formally recommended by the IS Director and approved by the County Manager as needed.

Note: Certain legacy applications may use older security and communication protocols which do not fully comply with advanced security practices. These systems will be upgraded as budget allows.

7. NON-COMPLIANCE

Since it is impossible to specify every instance that might result in a violation of the (IS) Information Technology Policy and the Related Standards listed on the chart on page 1, a standard of reasonableness will apply to determine whether a user's use of technology is unacceptable.

Violations of these standards may include one or more of the following:

1. Disciplinary action according to applicable County policies;
2. Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
3. Termination of employment; and/or
4. Legal action

REVISION HISTORY

Version ID	Revision Date	Author	Reason for Revision
V.1.0-2020		IS Technical Writer	BOC Approval