CHESTERFIELD COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES

Department:	**Information Systems Technology**	**Policy Number:**	**7-4**
Subject:	**Laptop and Mobile Storage Device Policy**	**Supersedes:**	
		Date Issued:	**03/01/09**

I. INTRODUCTION

Chesterfield County supports the use of county-issued laptops and mobile-storage devices. These mobile resources may be used to collect, transport or store county information. It is critical that laptops and mobile storage devices are protected in a manner consistent with the information-protection principles outlined in the county's information security policies.

A. Purpose

This policy is designed to reduce the risk associated with the loss or inappropriate use of county information. Specific threats that this policy addresses include, but are not limited to, unauthorized access, inappropriate disclosure, or loss of information associated with use of portable laptops and mobile storage devices.

Use of laptops and mobile storage devices may involve the creation of Chesterfield County information, which may be subsequently gathered, stored, or shared on those resources. It is necessary to identify appropriate security controls and define the proper use and handling of these mobile resources to ensure the protection of the information that may be stored on those extended computing resources.

B. Scope

This policy applies to, but is not limited to all individuals and entities using laptops and mobile storage devices for county business whether they are full-time or part-time employees, interns, temporary workers, volunteers, consultants, contractors, or other entities that have been contracted to perform work on behalf of Chesterfield County.

Employees are encouraged to not put county sensitive data on non-county devices. Information identified as sensitive that must be stored off-site shall be encrypted. If there is a need for remote computing needs, the employee should discuss those needs with their department head.

II. POLICY Statement

It is the responsibility of all county laptop and other storage device users to follow the computing guidelines as outlined in this policy to ensure county data is safeguarded appropriately.

Failure to comply with this policy associated with the use of laptops and mobile storage devices may result in disciplinary action up to and including termination.

Exceptions to this policy must be approved in writing by the requestor's department head or designee and the Chief Information Officer (CIO) or designee.

III. Responsibilities

A. Department Heads and Constitutional Officers

Department heads will have the responsibility to ensure appropriate use and handling of laptops and mobile storage devices. Primary responsibilities include:

1. Department heads or designees will approve acquisition and issuance of department laptops and mobile storage devices
2. Where possible, ensure that information is not stored by staff on mobile devices. Mobile workers should connect via VPN or other IST approved secure connection to manage county work products.

B. Laptop and Mobile Storage Device Users

Laptop and mobile storage device users will:

1. Ensure the physical protection of the laptop or mobile storage device that has been assigned to them.
2. Re-certify annually by completing Information Security Awareness training.
3. Connect weekly to the county network to ensure that appropriate security patches are applied to the laptop or mobile storage device.
4. Public Safety Mobile Data Computer (PMDC's) users are subject to specific Public Safety guidelines on the use and care of those devices.

C. Information Systems Technology (IST)

1. Information Systems Technology (IST) will take reasonable safeguards to ensure protection against inadvertent or intentional disclosure, unauthorized information manipulation, accidental, or deliberate deletion of county information created, or stored on laptop computers, or other mobile storage devices.
2. IST is responsible for review and approval of requisitions for hardware, software and other technology solutions prior to purchase.
3. IST is responsible for the secure installation, configuration, distribution, management and removal from service of laptops and mobile storage devices and associated security software unless authority has been approved for delegation to a non-IST support group.
4. IST reserves the right to monitor usage of laptops and mobile storage devices. The IST security services section is responsible for monitoring the mobile environment for security compliance and response to information-security related incidents.
5. IST will manage local administrator rights to be restricted from use on mobile resources unless requested in writing by the mobile user's respective department head and approved by the CIO as an exception.

IV. TECHNICAL Controls

A. Minimum Technical Safeguards

The following minimum technical safeguards shall be implemented in the mobile environment:

1. Mobile resources will be configured in accordance with accepted Information Systems Technology mobile-computing configuration standards.
2. Mobile users will have non-administrative rights to the mobile device.
3. All mobile resources will be required to connect via an authenticated, encrypted session to the county network in order to create, access, share, or store information on the county network.
4. Mobile resources will be configured to log, where possible, significant security relevant events (such as unauthorized login or access attempts, account lock-outs, etc.)
5. Laptops and mobile storage devices used to temporarily store or transport sensitive information must utilize IST-approved encryption methods to ensure that information cannot be read as clear-text.

V. definitions

Laptop
A portable computing device.

Mobile Storage Device
A portable device intended to collect or store information that has storage and/or media playback capability. Typical examples of mobile storage devices include, but are not limited to, removable media (e.g., jump drives, thumb drives, compact discs, etc.) and media players (such as MP3 players).

Sensitive Information
Sensitive information may be confidential in nature and includes other information for which access should be restricted or controlled based upon related county policy, laws or regulations.

Confidential Information

Confidential records are public records which are generally not made available for public inspection, due to reasons of federal, state, or county laws, ordinances, regulations, or court orders ensuring and requiring the privacy of information - usually of a personal nature- contained within them.

Criteria for determining if a record should be maintained as confidential include, but are not limited to:

- If the record could cause malicious harm to the physical well-being or reputation of the Public Schools, County government, to any employees, or to any citizens;
- If the record could compromise public safety;
- If the record would give an unfair advantage to one party in a commercial transaction;
- If the record was created under an understanding of attorney-client privilege;
- If the record has a bearing on an ongoing internal, civil, or criminal investigation or audit;
- If the record is protected under one or more federal, state, or local laws, regulations, or ordinances;
- If the record contains personal healthcare information;
- If the record contains information of a personal nature that could be linked to or traced to a person.

Examples of Confidential Information

HIPAA - *HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Public Law 104-191, 145 CFR Part 160*

- Protected data when associated with a health record Patient name(s)
- Street address, city, county, zip code
- Dates (except year) related to an individual
- Social security numbers
- Health conditions/symptoms
- Prescriptions
- Account/medical record numbers
- Health plan beneficiary information
- Certificate/license numbers
- Vehicle ID and serial numbers
- Device IDs and serial numbers
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic or code
- Payment guarantor's information
- Telephone/fax numbers
- E-mail, URLs or IP addresses

FERPA - *Family Educational Rights and Privacy Act, 34 CFR Part 99*

- Individual student records
- Grades
- Courses taken
- Schedule
- Test scores
- Advising records
- Educational services received
- Disciplinary actions
- Student ID number
- Social security numbers
- Student private e-mail

(GLB) Data - *Gramm-Leach-Bliley Act, 15 USC, Subchapter I, Sec. 6801-6809, Disclosure of Nonpublic Personal Information*

- Employee financial account information
- Student financial account information – aid/grants/bills
- Individual financial information
- Business partner and vendor financial account information

Employee Information

- Social Security number
- Date of birth

- Home address or personal contact information
- Performance reviews
- Specific benefit selections
- Sexual harassment complaints/investigations/findings
- Employee Relations records
- Drug and Alcohol testing information
- Background investigations
- Grievance information
- Payroll information
- Discrimination complaints/investigations/findings

Attorney/client privileged records
- Trade secrets, intellectual and/or proprietary research information
- Information required to be protected by contract
- Adoptions
- Pending litigation documents

Restricted police records
- Victim information
- Juvenile records
- Investigations from Internal Affairs offices
- Jail records dealing with riots, escape, and/or emergency evacuation procedures
- Undercover police identities, contacts, and activities
- Accidents

General records
- Donor information
- Library use records
- Anonymous contributions
- Deposit information
- Medical/mental health records
- Most records relating to juveniles
- Tax returns
- Personal identifying information
- Information your department has deemed confidential