COURT PERSONNEL POLICY
NUMBER 1 OF 2006
July 1, 2006

ELECTRONIC MEDIA, EMAIL & INTERNET

INTRODUCTION: In recognition of the Court of Common Pleas of Washington County's constitutional authority to direct its workforce to ensure the efficient administration of justice, and the Court's interest in continuing its amicable relationship with the County, the Court promulgates this policy to provide all court-appointed employees direction on the proper use of electronic media, email and the Internet. This policy applies to all court-appointed employees. All computer hardware and software is the property of the Court and the County and all electronic media, email and Internet access will be periodically reviewed by the District Court Administrator or the Court's Designee in conjunction with the Court Automation Department. Employee use of the Court and County computer systems creates consent to the monitoring of that use by the Court.

ELECTRONIC MEDIA

OWNERSHIP OF INFORMATION STORED ON ELECTRONIC MEDIA

DEFINITIONS:

Court Information – includes all case information; court documents; reports; memoranda; policies; court, court-related or juror databases; email; Court Automation management reports; or any other information created by court personnel or by others for the benefit of the court.

Court Employee – For purposes of this policy the term includes any court-appointed employee.

Authorized Use – Use of the Computer Hardware or Software, Internet Access or Email privileges for purposes not associated with official Court business as permitted by this policy.

SECTION I. OWNERSHIP OF COURT INFORMATION STORED ON ELECTRONIC MEDIA

All **Court Information** in any format, stored by any means on Court or County-owned electronic facilities (Voicemail, Email, computer network drives, hard disks, CD's or individual diskettes, etc.) is the property of the Washington County Court of Common Pleas. In keeping with the Independence of the Judiciary, no Court Employee, as defined above, shall distribute **Court Information** without proper authorization of the Court. No Court Employee has any right to privacy in the use of the Court or County Computer system. No Court Employee may install any hardware or software on a Court or County Computer system without the express written consent of the Court, or District Court Administrator, and the Court Automation Department Director. The installation of hardware or software on Court Computers or Computer Systems will be coordinated with the County Information Technology Department, but the Court retains the final approval authority for the installation of the hardware or software.

SECTION II. ACCESS AND MONITORING USE

Court Automation or County Information Technology Department personnel may, at the direction of the Court, the District Court Administrator, or the Court's designee, access a Court Employee's files. Unless otherwise directed by the Court, any and all reports or information regarding **Court Information** or reports concerning usage of computers or the Internet by Court Personnel is confidential, and will only be shared between Court management and the member(s) of the Court Automation and County Information Technology Department from whom the information or reports were requested.

SECTION III. CORRECTIVE AND DISCIPLINARY ACTION

Violation of this policy may result in disciplinary action and suspension of Network, Voicemail, Email, or Internet access. In addition, criminal prosecution and civil liability may apply to certain actions outside the scope of an employee's official duties.

EMAIL

SECTION I. EMAIL PROCEDRES

A. All email messages produced by Court Employees on Court or County-provided systems are the property of the Washington County Court of Common Pleas. Email will be used only for business purposes and authorized use.

B. Email messages and attachments are neither secure nor private. Email messages can be retrieved by anyone with access to a user's password, access rights, or computer while the user is logged on.

C. Individual users must be aware of and at all times comply with the following standards:

1. Every Court Employee is responsible for ensuring that posted messages are professional and businesslike and have the Court's best interests in mind. Remember that these guidelines apply to personal expressions as well. If email communications are taken out of context or misinterpreted, they can have an unplanned and negative impact on the Court, or they may be misconstrued as official endorsements or statements.
2. Email communications should be drafted with the same care as a formal memorandum.
3. The contents of email communications should not include anything that the sender would not want publicly disclosed.
4. Email should not be used to discuss legally-protected, confidential or sensitive information. Failure to comply with State and Federal law and regulations on these matters may result in punishment in accordance with those State and Federal laws and regulations.
5. Court Employees are strictly prohibited from sending Email messages of a harassing, intimidating, indecent, defamatory, offensive or discriminatory nature, including the creation, display or transmission of sexually explicit images, cartoons, jokes, messages, vulgarities, or obscenities.
6. Every Court Employee is required to ensure that access to the Court or County computer system is restricted to other employees and authorized users. Unauthorized access to another employee's files or use of the employer's facilities to gain unauthorized access to other employer or non-employer computing facilities is a major breach of security and ethics and may subject the employee to discipline, including termination from employment.

D. No person, including Court Automation or County Information Technology personnel, shall access, read, alter, or delete any other person's email without specific authorization from the Court, District Court Administrator, the Court's Designee or individual user. All reports of either a summary or detailed nature produced by Court Automation or County Information Technology personnel are confidential, and may be shared, shown, and discussed only with Court management personnel, or otherwise as directed by the Court or the District Court Administrator.

E. Email may be used for appropriate Court-related business in accordance with the guidance listed in paragraph C above and for authorized use. Authorized use includes email communication that:

1. Serves a legitimate public interest,

2. Does not adversely affect the performance of official Court duties,

3. Is of reasonable duration and frequency, and whenever possible, is made during personal time (such as during break time and lunch time),

4. Does not overburden the communication system,

5. Does not create additional costs to the Court or the County,

6. Does not reflect adversely on the Court or the County, and

7. Does not conflict with the interest of the Court.

F. Examples of Authorized Use include, but are not limited to:

1. Brief communications with family members to exchange important and time-sensitive information; such as scheduling doctor, automobile, or home repair appointments.

2. Educating or enhancing the professional skills of employees (e.g., use of communication systems, work-related application training, etc.)

G. The following do not constitute Authorized Use and are prohibited.

1. Distributing copyrighted materials by email or email attachments without consent from the copyright owner. Failure to maintain consent may violate federal copyright infringement laws and could subject the individual to civil liability or criminal prosecution,

2. Sending or receiving email for commercial or personal financial gain,

3. Intentionally or unlawfully misrepresenting your identity or affiliation in email communications,

4. Using someone else's identity (UserID) and password without proper authority,

5. Sending or forwarding chain letters, broadcasting inappropriate messages to groups or individuals, or otherwise causing congestion on the network,

6. Sending or forwarding material that expresses or promotes discriminatory attitudes based upon religion, gender, age, nationality or other similar groups, and

7. Intentionally or unlawfully sending or forwarding software used for "hacking" or "cracking" internal or external computer systems such as viruses, mail bombs, and the like.

H. Violation of this policy may lead to disciplinary action and/or loss of Email and/or Internet access.

INTERNET ACCESS & USE

SECTION I. RULES FOR INTERNET USE

A. Court Employees will use Internet access for Court-related business or Authorized Use only. All Internet access shall comply with applicable law and policies. Intentional misuse may subject the user to termination of access rights and to disciplinary action.

B. **Any and all material downloaded from the Internet shall be downloaded to the user's local accessible hard drive to avoid contamination by computer viruses.** No files should be copied to any network drive until the files have been scanned for computer viruses.

C. Each user must maintain password confidentiality. Users will neither share any password for any computer or network facility with any unauthorized person, nor obtain any other user's password by unauthorized means.

D. No person (including Court Automation and Information Technology Department personnel) shall access, read, alter, or delete any other person's computer files or email without specific authorization from the Court, District Court Administrator, the Court's Designee, or individual user.

E. Court Employees are specifically prohibited from:

1. Any use of the Court or County provided computer hardware or software for other than Court-related business or Authorized Use.

2. Activities for personal or commercial gain. This includes, but is not limited to, chain letters; commercial solicitation; and sales of personal property.

3. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, "hate literature," such as racist literature, materials or symbols (for example, swastikas, neo-Nazi materials, and so forth), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

4. Accessing inappropriate web sites (unless for investigatory purposes and approved in advance for these purposes), including, but not limited to, those related to: pornography, drugs, gambling, games, information technology-hacking, information technology-proxy avoidance systems, chat rooms, open forum discussions, militancy/extremism, racism/hate, and violence.

5. Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

6. Using another person's account or identity without appropriate authorization or permission.

7. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

8. Attempting to circumvent or defeat security or auditing systems.

9. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

10. Permitting any unauthorized individual access to the Court or County system.

11. Streaming.

F. Authorized Use. Court Employees may access appropriate websites via the Internet as long as this access is limited in scope and duration and is conducted during the Court Employee's break or lunch period. Appropriate websites include, but are not limited to, bank websites to balance a checkbook; news, weather, and sports websites. Court Employees may not subscribe to non-Court related news sites.

SECTION II. MONITORING AND REPORTING USE

No one, including Court Automation and County Information Technology Department personnel, may monitor the usage of the Internet by Court Employees except as directed by the Court, District Court Administrator, or the Court's Designee. All reports of either a summary or detailed nature produced by Court Automation or County Information Technology Department are confidential, and may be shared, shown and discussed only with Court management personnel, or otherwise as directed by the Court. To the limited extent necessary to ensure the Court maintains reasonable and necessary computer capabilities, the County Information Technology Department may monitor general bandwith use on the T-1 line(s) that service the Family Court Center and the Courthouse. In the event that bandwith use begins to cause or is likely to begin to cause difficulties in the operation of the Court Computer Systems or the County Computer Systems, this fact shall be communicated to the Court Automation Department. Once this issue is communicated to the Court Automation Department, the Court, the District Court Administrator, or the Court's Designee, will determine and may authorize the review of the specific cause(s) of the bandwith issue(s). The County Information Technology Department is not authorized to determine the specific cause of the bandwith issue(s) without prior approval of the Court, the District Court Administrator, or the Court's Designee.

SECTION III. SANCTIONS FOR VIOLATIONS

Violation of this policy may lead to disciplinary action and/or loss of Internet access.

In the event of a serious virus outbreak, or in the event of repeated breaches of this policy by a department's personnel, that department's personnel will be disconnected from the Internet and the County Wide Area Network until compliance with this policy is re-established and all viruses are removed.

I have received a copy of the Court Electronic Media, Mail and Internet Policy dated July 1, 2006, and I have reviewed it. I understand that my failure to follow the guidance in this policy may lead to administrative action, up to and including termination of employment, may be taken against me.

_____ _____

Date Signature

_____

Printed Name