POLICY:

Chatham Area Transit Authority's email system is the sole property of the Authority and intended for use by authorized users for Authority business purposes only, although limited personal use is permitted consistent with this Policy. The Authority reserves the right to monitor all email. Use of the Authority email system must be consistent with the Authority's Values and Code of Business Conduct and the guidelines set forth below.

GUIDELINES:

To establish guidelines and educate authorized users on the responsibilities for use of the Authority email system and to improve the efficient use of the email system consistent with the Authority's Values.

General:

The following outlines the policy of the Authority with respect to the use of the Authority email system. All persons (including but not limited to employees, consultants, and others working with the Authority) who are authorized to use the Authority's email system are required to comply with this policy. Failure to comply can result in disciplinary action up to and including termination from employment.

Business Use. The Authority email system is intended to be used for business purposes of the Authority only. Limited personal use of email is allowed if (a) it is used in reasonable amount and without interference to work performance or business needs, (b) is not used for any unlawful, harassing, or immoral purpose, and (c) it is otherwise used in compliance with this policy. Specifically, without limitation, the use of the Authority's email system to send mass mailings, chain letters, junk mail, jokes and executables is strictly forbidden.

Ownership. All email accounts and all email content created, sent, received or stored on the Authority's email system, whether business or personal, are the sole property of the Authority and are not the property of the employee or other personnel.

Email Review. All email is subject to the right of the Authority to monitor, access, read, delete, copy, disclose and use such email without prior notice to the originators and recipients of such email. Email may be monitored and read by authorized personnel for the Authority for any violations of law, breaches of Authority policies, communications harmful to the Authority, or for any other reason.

No Presumption of Privacy/Confidentiality. Email communications should not be assumed to be private and security cannot be guaranteed. Highly confidential or sensitive information should not be sent through email. Users are required to use email in a manner that will not risk the disclosure of Authority proprietary and other information to persons outside the Authority.

Email Content. Emails should be professional, courteous and in compliance with all applicable laws. All emails should contain the sender's name, title and contact information.

Prohibited Acts. Provided below is a non-exclusive list of prohibited acts associated with the use of the Authority's email system. When considering the appropriateness of engaging in a particular act, users should be guided by both the specific prohibitions and the other mandates set forth in this policy.

Prohibited activities include:

- Using any words, images or references that could be viewed as libelous, offensive, harassing, illegal, derogatory, discriminatory, or otherwise offensive.

- Creating or transmitting email or images that might be considered inappropriate in the workplace, including, but not limited to, messages or images that are lewd, obscene, sexually explicit, or pornographic.

- Creating or transmitting messages or images that might be considered inappropriate, harassing or offensive due to their reference to race, sex, age, sexual orientation, marital preference, religion, national origin, physical or mental disability, or other protected status.

- Downloading, copying or transmitting documents or software protected by third party copyrights in violation of those copyrights. Any personnel with a question concerning a copyright issue should contact the IT or Legal Department.

- Using encryption devices and software that have not been expressly approved by the Authority.

Security. The email system is only to be used by authorized user, who have been issued an email and password. Personnel shall not disclose their codes or passwords to others or may not use someone else's code or password without express written authorization from an authorized officer of the Authority. Use of the email system by unauthorized persons is strictly forbidden.

Protecting the Attorney-Client Privilege. A confidential communication between a client and an attorney is privileged if it is made for the purpose of seeking, obtaining or providing legal advice or assistance. The purpose of the privilege is to promote the administration of justice by allowing individuals and businesses to seek legal advice without fear that their communications will be disclosed to others without their consent. Merely copying a lawyer on a memo or email does not create the privilege. The communication must be made in the course seeking or obtaining legal advice or representation.

The general rule as to who within the Authority is entitled to invoke the privilege includes only those persons within the Authority whose responsibility or involvement in a particular matter is such that a decision would not normally be made without that individual's input. If the communication is distributed to a larger group than fits this description the privilege can be lost to the entire group.

Therefore, communications intended to be privileged should be distributed to only those who need to be involved in the decision or controversy. Re-copying or forwarding a privileged communication to a broader group may cause the privilege to be lost. When in doubt about a particular email recipient, delete that person from the distribution list and consult the applicable Chief Financial Officer, Chief Operating Office, Chief Development Officer or the CEO.

Any communication that a sender seeks to protect should be labeled as "Confidential Attorney- Client Privileged" and its distribution limited as much as possible. Never forward email or documents labeled "Attorney-Client Privileged" without first consulting with the Legal Department.

Reporting. Authority personnel who are aware of the violation of this policy by another person should report the violation to a supervisor immediately.

Message Retention and Creation. Employees should be careful in creating email. Even when a message has been deleted, it may still exist in printed version, be recreated from a back-up system, or may have been forwarded to someone else. Please note that appropriate electronic messages may need to be saved. And, the Authority may be required to produce email in litigation. Strict adherence to any directives of the Legal Department or Senior Management to preserve email content is required.

Viruses. Care must be taken to avoid downloading of any viruses. Any files downloaded from email received from non-Authority sources must be scanned with the Authority's virus detection software. Any viruses, tampering or system problems should be immediately reported to the computer systems administrator.

Other Policies. All existing Authority policies apply to employee conduct in connection with email, including but not limited to, Authority policies regarding intellectual property, insider trading, misuse of Authority property, discrimination, harassment, sexual harassment, information, data security, and confidentiality.

Email Retention Upon Termination of Employment. Email retained on the Authority email system is the property of the Authority and users are forbidden to delete email from the system before or upon leaving the employment of the Authority.

Retention in the Event of Litigation, Subpoena, or Regulatory Inquiry. It is the Authority's policy to comply with all legal proceedings. In the event of any litigation, subpoena, regulatory inquiry, criminal proceeding, or the like, Authority users are absolutely

and unequivocally prohibited from deleting, discarding, or destroying any emails or any other documents relating in any way to the litigation, subpoena, regulatory inquiry, criminal proceeding, or the like.

No Waiver. Any delay or failure to discipline personnel for violations of this policy will not constitute a waiver of the Authority's rights.

Consequences of Violations. Violations of this policy or other Authority policies may result in discipline, suspension, termination of employment, and/or legal action.

Our Values. More simply put, the use of the Authority email system should at all times be consistent with Chatham Area Transit Authority's Values and Code of Business Conduct.

Questions. If you have any questions concerning this Email Policy, please contact the applicable CFO, COO, CDO or CEO.

APPLIES TO:

All employees of Chatham Area Transit Authority.