Book	Board of Trustees Policy
Section	800 Operations
Title	Acceptable Use and Internet Safety
Code	802
Status	Active
Adopted	August 1, 2016

Agora Cyber Charter School
1018 W 8th Ave
King of Prussia PA 19406

Board of Trustees

Acceptable Use and Internet Safety

The Agora Cyber Charter School ("Agora") Board of Trustees ("Board") provides computer network, equipment, tools, and Technology Resources to enhance educational opportunities for Agora students, employees, and the Agora community. This policy details acceptable use of Technology Resources provided by Agora. Agora provides these services and equipment a privilege, not a right, to the User (as defined below).

It is every Technology Resource User's duty to use Technology Resources responsibly, professionally, ethically and lawfully. Access to these resources may be designated a privilege, not a right. This policy applies to aspects of both adult and minor acceptable use of Technology Resources.

This policy is intended to fulfill requirements of state and federal laws to the extent applicable, including the Federal Children's Internet Protection Act (CIPA); 47 U.S.C. §§ 254(h) & (l); the Neighborhood Children's Internet Protection Act (NCIPA); and the 2008 Broadband Improvement Act, P.L. 110-385, including any applicable implementing regulations.

This policy addresses the following:
A. Access by minors to inappropriate matter on the Internet and World Wide Web;
B. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

C. Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online;
D. Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
E. Measures designed to restrict minors’ access to materials harmful to minors.

In using or accessing Agora’s Technology Resources, Users must comply with the following provisions:

Definitions
For the purposes of this policy, related procedures and forms, the following terms are defined as follows:

A. Child Pornography. Under federal law, any visual depiction, including any photograph, film, video, picture, or computer image or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C. § 2256(8)

B. Child Pornography. Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

18 PA CSA §6312(d)

C. Minor. Under CIPA, an individual who has not yet attained the age of seventeen is a minor. For other purposes, minor shall mean any person under the age of eighteen (18).

D. Obscene. Under federal and Pennsylvania law, any material if:

1. the average person, applying contemporary adult community standards, would find that the material, taken as a whole, appeals to the prurient interest;
2. the subject matter depicts or describes sexual conduct in a patently offensive way; and
3. the subject matter, taken as a whole, lacks serious literary, artistic, political or scientific value.

Miller v. California, 413 U.S. 15 (1973).

E. Password. A unique word, phrase, or combination of alphanumeric and non-alphanumeric characters used to authenticate a User ID as belonging to a specific User.

F. Sexual Act and Sexual Contact. Has the meanings given such terms under 18 U.S.C. §§ 2246(2) & (3), and 18 Pa.C.S. § 5903.

G. Technology Protection Measure. A specific technology that blocks or filters Internet access to content that is Obscene, Child Pornography or harmful to Minors and the material is covered by a certification regarding CIPA.

H. Technology Resources. Technologies, devices, and resources used to access, store or communicate information. This definition includes, but is not limited to, computers, information systems, networks, laptops, iPads, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audio-visual equipment, digital cameras, wireless reading devices, i.e. Kindles and Nooks, Internet, electronic mail, electronic communications, devices and services, multi-media resources, hardware and software, including Moodle software.

I. User. Any person who has signed this policy and is permitted by Agora to utilize any portion of Agora's Technology Resources including, but not limited to, students, parents, employees, Board members, contractors, consultants, vendors and agents of Agora.

J. User Identification (ID). Any identifier that would allow a User access to Agora's Technology Resources or to any program including, but not limited to, email and Internet access.

K. Vandalism. Any malicious attempt to harm or destroy Technology Resources, data of another user, the Internet or other networks. This includes, but is not limited to, the uploading or creation of computer viruses.

Authorized Users

Any authorized User may use Agora's Technology Resources. If a potential User has a history of discipline problems involving Technology Resources, the CEO or his designee may decide not to give the potential User access to certain Agora Technology Resources.

User Privacy

Computer accounts and Technology Resources are given to Users to assist them in the performance of Agora related functions. A User does not have a legal expectation of privacy in the User's electronic communications or other activities involving Agora's Technology Resources including email and anything they create, store, send, share, access, view or receive on or through the Internet.

By using Agora's network and Technology Resources, all Users are expressly waiving any right to privacy and consenting to having their electronic communications and all other use accessed, reviewed, and monitored by Agora. A User ID with email access will only be provided to authorized Users on condition that the User consents to interception or access to all communications accessed, sent, received or stored using Agora technology and signs this policy.

Electronic communications, downloaded material, and all data stored on Agora's Technology Resources, including files deleted from a User's account, may be intercepted, accessed, or searched by Agora administrators or designees at any time in the regular course of business to protect Users and Agora's equipment. Any such search, access, or interception will be reasonable in inception and scope and shall comply with all applicable laws.

Technology Administration

The Board directs the CEO or his designee to assign trained personnel to maintain Agora's technology in a manner that will protect Agora from liability and will protect confidential student and employee information retained on or accessible through Agora's Technology Resources.

Administrators may suspend access to and/or availability of Agora's Technology Resources to diagnose and investigate network problems, potential violations of the law, or Agora policies and procedures. All Agora Technology Resources are Agora property.

Agora may maintain or improve Technology Resources at any time. Agora or authorized Agora agents may remove, change or exchange hardware, equipment or other technology between buildings, classrooms, or Users at any time without prior notice.

Content Filtering and Monitoring

Agora employs a Technology Protection Measures as required by law. Agora will monitor the online activities of Minors on the Agora network and/or all Technology Resources and equipment with Internet access. At a minimum technology protection is meant to block visual depictions that are obscene, illegal, pornographic, child pornography and/or harmful to Minors, as well as Internet/World Wide Web computer access to such material. Users finding a website deemed inappropriate must report the website to the Agora IT department. After review of the website, Agora will take appropriate steps to block inappropriate site from Users.

For purposes of bona fide research or other lawful purposes, the CEO may make certain blocked sites available for those purposes only after approval of the request.
In making decisions to disable Agora's Technology Protection Measures, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit Agora. A student or parent/guardian claiming they have been denied access to Internet material not within the purview of this policy shall be afforded expedited review and resolution of the claim upon written notice to the CEO.

Technology Protection Measures are not foolproof, and Agora does not warrant the effectiveness of Internet filtering except to the extent expressly required by federal and state laws. Evasion or disabling, or attempting to evade or disable, a Technology Protection Measure installed by Agora is prohibited.

Agora shall not be held responsible when a student or other User knowingly or willingly accesses inappropriate material or communicates or shares such materials with others.

Viruses

Viruses can cause substantial damage to Technology Resources. Users are responsible for taking reasonable precautions to ensure they do not introduce viruses to Agora's Technology Resources.

All material received on disk, flash drive, or other magnetic or optical medium, and all materials downloaded from the Internet, Technology Resources, or networks that do not belong to Agora must be scanned for viruses and other destructive programs before being transferred to Agora's Technology Resources. Any User receiving an email from a questionable source must contact the Agora IT department before opening the email or any attachment included in the email.

To ensure security and avoid the spread of viruses, Users accessing the Internet through Technology Resources attached to Agora's network must do so through an approved Internet firewall or Technology Protection Measure.

Encryption Software

Users shall not install or use encryption software on any Agora Technology Resource without first obtaining written permission from the CEO. Users shall not use passwords or encryption keys that are unknown to the CEO.

The federal government has imposed restrictions on export of programs or files containing encryption technology. Software containing encryption technology shall not be placed on the Internet or transmitted in any way outside the United States.

Web Content Developed By Students

As part of class/course assignments, students may be developing and/or publishing content to the Internet via web pages, electronic and digital images, blogs, wikis, podcasts, vodcasts, and webcasts, or may be participating in video conferences.

The following guidelines must be adhered to when students develop and publish information to the Internet:

A. Personal information such as phone numbers, addresses, email addresses or other specific personal information shall not be published or shared to a public page or video conference.
B. All web content must comply with this policy.
C. All web content and video conferencing must be used under the direction and supervision of the teacher/administrator for educational purposes only.
D. All web content is subject to copyright law and fair use guidelines.
E. All web content shall only be posted to Agora approved web pages, blogs, wikis, podcasts, webcasts, vodcasts and videoconferences.

Prohibitions

Students, staff, and all Users are expected to act in a responsible, ethical and legal manner in accordance with Agora policies and federal and state laws. Specifically, the following uses of Agora's Technology Resources are prohibited:

A. To facilitate illegal activity, including unauthorized access and hacking;
B. To engage in commercial, for-profit, or any business purposes, except where such activities are otherwise permitted or otherwise authorized;
C. Non-work or non-school related work;
D. Product advertisement or political lobbying;
E. Production or distribution of hate mail, unlawfully discriminatory remarks, and offensive or inflammatory communication;
F. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials;
G. To access or transmit material that is harmful to Minors and/or Users, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property;
H. Use of inappropriate language or profanity;
I. To transmit material likely to be offensive or objectionable to recipients;
J. To intentionally obtain or modify files, data and passwords belonging to other Users, or integral to system and network operations;
K. Impersonation of another User, anonymity and/or use of pseudonyms;
L. Loading or use of unauthorized games, programs, files, or other electronic media;
M. To disrupt the work of other Users;

N. Destruction, modification, or abuse of Technology Resources and peripheral hardware or software;
O. Relocation of Agora hardware without prior administrative consent;
P. Quoting personal communications in a public forum without the original author's prior consent;
Q. To access or use any form of electronic mail on Agora Technology Resources unless authorized by the CEO or his designee;
R. Using the network to participate in online or real-time conversations unless authorized by the teacher/administrator for the purpose of communicating with other classes, students, teachers, experts or professionals for educational purposes;
S. Using a disk, removable storage device or CD/DVD brought into Agora from an outside source that has not been properly scanned for viruses or authorized for use by a teacher/administrator in accordance with Agora established procedures;
T. To discriminate against, advocate violence against, harass, intimidate, bully or cyberbully others;
U. To send unsolicited (“spamming”) or forwarded emails and chain letters to persons;
V. Using “spoofing” or other means to disguise User identities in sending email or other electronic communication via bulletin boards, newsgroups, social networking sites, instant messages, email systems, chat groups, chat rooms, or through other Technology Resources;
W. To send, transmit or otherwise disseminate proprietary data, trade secrets, or other confidential information of Agora;
X. Posting or allow the posting of personal information about themselves or other people on the Technology Resources unless authorized by the CEO.Personal information includes address, telephone number (including home, work and cell phone numbers), school address, work address, pictures or video bites, clips, etc.;
Y. To refer to or attempt to refer to Agora or its employees, agents, Board, parents or students in any electronic communication, posting, blog, website, email or social networking site, without written authorization of the CEO;
Z. To access or transmit gambling, pools for money, or any other betting or games of chance;
AA. To solicit information with the intent of using such information to cause personal harm or bodily injury to another or others;
BB. Posting, sharing or attempting to post information that could endanger an individual, cause personal damage or a danger of service disruption; and
CC. Indirectly or directly making connections that create “backdoors” to Agora, other organizations, community groups, etc. that allow unauthorized access to the Technology Resources or Agora.

Security

Agora intends to strictly protect its Technology Resources against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these assets and in lessening the risks that can harm Technology Resources. Therefore, Users are required to comply fully with this Policy and immediately report any violations or suspicious activities to the CEO.

System security is protected in part by the use of passwords. All passwords must be at least eight (8) characters and include alphanumeric and special characters. Users will be required to change their passwords every thirty (30) days. Agora will maintain a password history that

prevents the use of a repetitive password. After three (3) unsuccessful access attempts, an attempted User will be locked out and must contact the CEO or his designee to regain access. After sixty (60) minutes of inactivity, the User will be automatically logged off the system.

Failure to adequately protect or update passwords could result in unauthorized access to personal or Agora files. Users shall be responsible for safeguarding their passwords for access to Agora's Technology Resources and for all transactions made using their passwords. To protect the integrity of Agora Technology Resources and systems, the following guidelines shall be enforced:

A) Students and other Users shall not reveal their passwords to another unauthorized individual.

B) Passwords shall not be printed or stored online.

C) Students and other Users are required to log off from the network when they complete working at a particular station.

D) Users are not to use a computer that has been logged in under another student's, teacher's or User's name.

E) Any User identified by the CEO or his designee as having a history of discipline problems involving Technology Resources may be denied access to any or all of Agora's Technology Resources.

F) Students and other Users shall not alter a communication originally received from another person or computer with the intent to deceive.

G) Users shall not misrepresent the identity of a sender or source of communication.

H) Users shall not disable or circumvent any Agora security; software or hardware.

I) Users shall not interfere with or disrupt Agora's systems, network accounts, services, or equipment.

J) Files, system security software/hardware or any Agora system shall not be altered or attempt to be altered without the written authorization of the CEO or his designee.

K) Unauthorized hardware and electronic devices shall not be connected to the Agora system.

L) Users shall comply with requests from the CEO or his designee to discontinue activities that threaten the operation or integrity of the Agora system.

Use of passwords to gain access to Technology Resources or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on Technology Resources. Agora retains access to all material stored on the Technology Resources regardless of whether that material has been encoded with a particular User's password, subject to limitations as set forth in Agora's policy governing Remote Access and Monitoring of Agora's Technology Resources, as well as applicable law.

Users shall not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users shall not use the Technology Resources to "snoop" or pry into the affairs of other Users by unnecessarily reviewing the files and emails of another.

A User's ability to connect to another computer's system through the network or by any other electronic means shall not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the administrators of those systems and the CEO.

Safety

To the greatest extent possible, Users of the network will be protected from harassment or unwanted or unsolicited communication. Any network User who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher, staff member or an administrator.

Communications through Agora Technology Resources are limited to only that which serves a demonstrable educational purpose. For safety reasons, Agora Users shall not reveal personal addresses or telephone numbers to other Users on Agora networks or on the Internet.

The CEO or his designee shall be responsible for implementing protection measures to determine whether Agora's computers, laptops, iPads, Kindles and other Technology Resources and technology related devices such as USB drives, digital cameras and video cameras, PDAs, MP3 players, printers, etc. are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include, but not be limited to:

A) Utilizing technology protection measures that block or filter Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by Minors, or determined inappropriate for use by Minors by the Board.

B) Maintaining a listing of all employees and Users with access to the room which contains Agora's server.

C) Generate and maintain monitoring reports (including firewall logs) of User activity and remote access on Agora's system by all Users, including but not limited to students, employees, contractors, consultants, and/or vendors.

i. The report should include the date, time and reason for access, whether it was remote access, changes made and who made the changes.

D) Maintaining documentation that students no longer enrolled at Agora, terminated employees, and contractors/vendors with expired contracts or who are terminated are properly removed from Agora's system in a timely manner.

E) Analyzing the impact of proposed program changes in relation to other critical business functions before adopting the proposed program changes.

F) Developing compensating controls to mitigate information technology (IT) weakness and alert Agora to unauthorized changes to student data, i.e. reconciliations to manual records, analysis of student trends, data entry procedures and review, etc.

Vendors

If Agora shares internally sensitive or legally/contractually restricted Agora data with parties outside the Agora community, Agora shall first enter into a Non-Disclosure Agreement with the party. The Non-Disclosure Agreement is needed to protect Agora's proprietary or otherwise sensitive information. Non-Disclosure Agreements are typically needed when entering into a business relationship with vendors, consultants, and contractors. Agora's legal counsel must review all Non-Disclosure Agreements before signing.

All vendors, consultants, and/or contractors shall only be granted access to Agora's Technology Resources to make changes or updates with prior written authorization from the CEO or his designee. Once the vendor, consultant and/or contractor, completes its work, access to Agora's Technology Resources will be removed.

Vendors, consultants and contractors are required to assign unique user IDs and passwords to each of their employees authorized to access Agora's system. Vendors, consultants and/or contractors may be terminated for violating this Policy and/or violating any state or federal laws.

All vendors, consultants and/or contractors and their employees, who have direct contact with students, must comply with the mandatory background check requirements for federal and state criminal history and child abuse. An official child abuse clearance statement for each of the vendors', consultants', and/or contractors' employees shall be submitted to Agora prior to beginning employment with Agora. Failure to comply with the background check requirements shall lead to immediate termination.

Closed Forum

Agora's Technology Resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law.

All expressive activities involving Agora Technology Resources that students, parents/guardians and members of the public might reasonably perceive to bear the approval of Agora and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of Agora for legitimate educational reasons. All other expressive activities involving Agora's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

Records Retention

Agora personnel shall establish a retention schedule for the regular archiving or deletion of data stored on Agora Technology Resources that complies with Agora's Record Retention and Destruction Policy as well as all federal and state laws and regulations. It is the User's responsibility to know which records are subject to these conditions and to comply with these laws and regulations or to contact the CEO for clarification.

In the case of pending or threatened litigation, Agora's attorney will issue a litigation hold directive to the CEO or his designee. A hold directive will direct all Agora administration and staff not to delete or destroy any electronic mail or other documentation on a computer as related to a specific student, employee, issue and/or for a specific time period. Failure to follow such a directive could result in negative legal consequences for the User and/or within the actual or threatened litigation. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by Agora's attorney.

Email and computer accounts of separated employees that have been placed on a litigation hold will be maintained by Agora until the hold is released. No employee, who has been so notified of a litigation hold, may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Drafting Emails

Like any other document, an email message and other computer information is discoverable during litigation. An email may be used in litigation to indicate what a User knew or felt. It is important to keep this in mind when creating emails and other documents. Even after you delete an email message or close a computer session, it may still be recoverable and may remain on the system. Since email communications are discoverable during litigation, they will have to be turned over to the opposing party unless determined to be privileged by Agora's legal counsel.

Privileged Attorney-Client Communications

Confidential email sent to or retained from counsel or an attorney representing Agora shall include this warning header on each page: "ATTORNEY CLIENT PRIVILEGED: DO NOT FORWARD WITHOUT PERMISSION."

Damages

All damages incurred by Agora due to a User's intentional or negligent misuse of Agora's Technology Resources, including loss of property and staff time, may be charged to the User. Agora administrators have the authority to sign any criminal complaint regarding damage to Agora technology.

No Warranty/No Endorsement

Agora makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides.

The electronic information available to students and staff on the Internet or through web-based services does not imply endorsement of the content by Agora, with the exception of resources approved and adopted by the Board. Nor does Agora guarantee the accuracy of information received using Agora's Technology Resources.

Agora is not and shall not be responsible for the loss of data, delays, nondeliveries, misdeliveries or service interruptions. Agora is not and shall not be responsible for any information that may be damaged or unavailable when using Agora Technology Resources or for any information that is retrieved via the Internet. Agora is not and shall not be responsible for any damages incurred as the result of using Agora's Technology Resources, including but not limited to, the loss of

personal property used to access Technology Resources. Further, Agora is not and shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other commercial online services.

Unauthorized Disclosure of Information of Minors

It is a violation of state laws, including, but not limited to Chapter 12 of Title 22 of the Pennsylvania Code, The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) and all other federal laws and regulations, to access data of a student the User does not have a legitimate educational interest in or to disclosure information about a student without parental permission or absent an exception to the disclosure requirements. Access and distribution of student data is recorded.

Questions regarding the disclosure of student information must be directed to the CEO prior to disclosure and must conform to Agora's student records and confidentiality policies. Unauthorized disclosure, use and dissemination of personal information regarding Minors is prohibited.

Compliance with Applicable Laws and Licenses

In their use of Technology Resources, Users must comply with all software licenses/copyrights and all other state, federal, and international laws governing intellectual property and online activities. Users shall not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the email system or by any other means unless it is confirmed in advance from appropriate sources that Agora has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by Agora, as well as legal action by the copyright owner. Any questions concerning these rights should be directed to the CEO or his designee.

Violations of Acceptable Technology Usage Policies and Procedures

Use of Technology Resources and equipment in a disruptive, manifestly inappropriate or illegal manner impairs Agora's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all Users granted access to Agora's Technology Resources. Any violation of Agora policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of User privileges. User privileges may be suspended pending investigation into the use of Agora's Technology Resources and equipment.

Employees may be disciplined or terminated, and students suspended or expelled, for violating this Policy. Any attempted violation of Agora's policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Consequences for Inappropriate Use

Agora Users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of Agora Technology Resources includes, but is not limited to: intentional copying, deletion or damage to files or data belonging to others; copyright violations; or theft of services. Any illegal usage of Agora Technology Resources will be immediately reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet or any Agora Technology Resource. Suspension of access, loss of access and other disciplinary actions may be consequences for inappropriate use. Vandalism may result in cancelation of access privileges, discipline and possible criminal action.

Cessation of Access

Upon termination or ending of enrollment, employment or the termination of any contract with or from Agora, no further access to or use of Technology Resources is permitted without the express authorization from the CEO.

Education of Technology Resource Users

Agora shall implement a program which educates students and staff about acceptable use and internet safety associated with Agora's Technology Resources. All students must complete a designated Technology Resources and Internet training prior to unsupervised use of Agora's Technology Resources as required by the 2008 Broadband Data Improvement Act. This training includes, but is not limited to: appropriate online behavior, including interacting on social networking websites and in chat rooms; cyberbullying awareness and response; proper use of Technology Resources; restricted activities with Technology Resources; and access and monitoring of school-issued Technology Resources to students.

No Additional Rights

This Policy is not intended for and does not grant Users any contractual rights. Users of Agora's Technology Resources must review this policy closely and sign and return to Agora a form acknowledging receipt and acceptance of the terms in this policy, which is attached hereto. Venue for any legal action arising out of an alleged and/or actual violation of the attached Agreement(s) shall be in Montgomery County, Pennsylvania.

TO THE EXTENT THAT ANYTHING IN THIS POLICY COULD BE CONSTRUED TO CONFLICT WITH AGORA'S CHARTER OR APPLICABLE STATE AND/OR FEDERAL LAWS, THE APPLICABLE STATE AND/OR FEDERAL LAWS AND/OR CHARTER CONTROL.