Note: For information regarding use of the District's technology resources and electronic communications by Board members, see BBI(LOCAL). For student use of personal electronic devices, see FNCE. For additional provisions governing employee use of electronic media, see DH(LOCAL) and the employee handbook. For information regarding District, campus, and classroom websites, see CQA. For information regarding intellectual property and copyright compliance, see CY.

GENERAL INFORMATION

The Superintendent or designee and the Chief Technology Information Officer will oversee the District's technology resources, meaning electronic communication systems and electronic equipment.

The District will develop and implement acceptable use guidelines covering acceptable use of the District's technology resources [see CQ(EXHIBIT)-B]. District employees and contractors can access the acceptable use policy for District technology resources on the Houston ISD employee portal.

FILTERING

The Superintendent will designate the Information Technology Security Officer (ITSO) to select, implement, and maintain appropriate technology for filtering material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on the District's network and computers.

INAPPROPRIATE MATERIAL

The following guidelines will apply:

1. The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to, nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and online gambling.

REQUESTS TO DISABLE FILTER

2. The ITSO will consider and maintain documentation of requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The ITSO will review and evaluate the risk, may consult as necessary, then decide regarding approval or disapproval of disabling the filter for the requested use. Requests to disable a filter should be e-mailed to HELPDESK@houstonisd.org.

ACCESS

Access to the District's technology resources will be governed as follows:

STUDENT ACCESS

1. Students in kindergarten–grade 12 will be granted access to the District's technology resources by the principal or designee, as appropriate.

2. Students are responsible for using their user ID and password when logging on to District computers and District-issued mobile devices.

STUDENT TRAINING

3. Students granted access to the District's technology resources must complete any applicable user training.

CLASS ACCOUNT

4. As appropriate and with the written approval of the immediate supervisor and completion of District network training, District employees will be granted access to the District's technology resources.

PASSWORDS

5. The District will require that all faculty and staff passwords be changed every 90 days. All passwords must remain confidential and should not be shared.

ACCESS DENIAL

6. Any user identified as a security risk or as having violated District and/or campus use guidelines may be denied access to the District's technology resources.

LIMITED PERSONAL USE

7. Resources are to be used mainly for educational and administrative purposes, but some limited personal use is permitted.

STUDENT PARTICIPATION IN SOCIAL MEDIA

Participation in approved social media sites using the District's technology resources for educational and administrative purposes is permissible for students under appropriate supervision.

Students participating in social media using the District's technology resources should assume that all shared content, including pictures, is public. No personally identifying information should be published. Students should not respond to requests for personally identifying information or contact from unknown individuals. Information about the date, time, and location of District field trips should not be shared. [See REPORTING VIOLATIONS, below]

DISCIPLINARY ACTION

The ITSO and principal will:

NOTICE

1. Notify the appropriate administrator of incidents requiring District response and disciplinary measures; and

MONITOR

2. Be authorized to monitor or examine all system activities, including campus-based social media, as deemed appropriate to ensure student safety online and proper use of the District's technology resources.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's technology resources:

PROTECTING ACCOUNT	1.	The individual in whose name an account is issued will be responsible at all times for its proper use and for not sharing the password for that account with others.
USING DISTRICT RESOURCES	2.	The District's technology resources may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
TAMPERING WITH DISTRICT PROPERTY	3.	Users may not access the resources to knowingly alter, damage, or delete District property or information or to breach any other electronic equipment, network, or electronic communications system in violation of the law or District policy.
VANDALIZING DISTRICT PROPERTY	4.	Users may not damage or vandalize electronic communication systems or electronic equipment, including knowingly or intentionally introducing a virus to a device or network, or not taking proper security steps to prevent making a device or network vulnerable, such as opening e-mail messages from unknown senders and loading unauthorized software.
DISABLING FILTERING PROPERTY	5.	Users may not disable, or attempt to disable, any filtering device used by the District.
ENCRYPTING	6.	Users may not purposely use encryption channels to avoid security review by system administrators except for appropriate business use as defined herein.
USING ANOTHER'S ACCOUNT	7.	Users may not use another person's account.
USING UNDER FALSE PRETENCE	8.	Users may not pretend to be someone else when posting, transmitting, or receiving messages.
TAMPERING WITH ELECTRONIC MEDIA	9.	Users may not attempt to read, delete, copy, modify, or interfere with another user's posting, transmittal, or receipt of electronic media.
HARASSMENT	10.	Users may not engage in conduct that harasses or bullies others. [See DIA, FFH, and FFI]
CYBERBULLYING	11.	Users may not send, post, or possess materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including cyberbullying and "sexting." Users who access such material are expected to discontinue the access as quickly as possible and report the incident to a supervising teacher and/or technology coordinator.
MAKING THREATS	12.	Students may not use e-mail or websites to engage in or encourage illegal behavior or to threaten school safety.

USING INAPPROPRIATE LANGUAGE	13. Users may not use inappropriate language such as ethnic or racial slurs or any other inflammatory language.
STUDENT INFORMATION	14. Students may not distribute personal information about themselves or others by means of the District's technology resources; this includes, but is not limited to, personal addresses and telephone numbers.
PERSONAL CONTACT	15. Students may not respond to requests for personally identifying information or contact from unknown individuals.
REQUEST FOR INFORMATION	16. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any request for such a meeting.
TRANSMITTING INFORMATION	17. Users may not post or transmit pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of 18.
INTELLECTUAL RIGHTS	18. Users must not violate intellectual property rights by redistributing copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
E-MAILS	19. Users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
SPAM	20. Users may not waste the District's technology resources, including sending spam, chain letters, and the like.
UNAUTHORIZED ACCESS	21. Users may not gain unauthorized access to resources or information.
VANDALISM	Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's technology resources or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer or network viruses.

ETIQUETTE

In addition to the standards for online conduct, users of the District's technology resources are expected to observe the following standards for etiquette:

- Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
- Be considerate when sending e-mail attachments by taking into account whether a file may be too large to be accommodated by the recipient's technology resources or may be in a format unreadable by the recipient.
- Do not use the District's technology resources in such a way that would disrupt use for others.

REPORTING VIOLATIONS

Students and employees must immediately report any known violation of the District's applicable policies or acceptable use guidelines to a supervising teacher or the technology coordinator.

REQUESTS FOR PERSONALLY IDENTIFIABLE INFORMATION

Students and employees must report to a teacher or an administrator requests for personally identifying information or contact from unknown individuals, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal to federal and state compliance.

SANCTIONS

Inappropriate use of the District's technology resources may result in suspension or revocation of the privilege to use these resources, as well as other disciplinary or legal action, in accordance with applicable laws, District policies, the Student Code of Conduct, and District administrative regulations.

TERMINATION / REVOCATION OF USE

Termination of access for violation of District policies or regulations will be effective on the date the principal or Superintendent or designee receives notice of withdrawal or of revocation of system privileges or on a future date if so specified in the notice.

DISCLAIMER

The following guidelines will apply:

1. Opinions, advice, services, and all other information expressed by users, information providers, service providers, or other third-party individuals are those of the providers and not the District.

COOPERATION WITH LAW ENFORCEMENT

2. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's technology resources and will cooperate fully with law enforcement in response to any investigation or valid subpoena. [See GR series]

CAMPUS REQUESTS FOR SOCIAL MEDIA	The District maintains a list of social media tools approved for use providing minimal security standards. To request access to a social media site (e.g., Facebook), a campus may submit a request to the District Helpdesk.
CONSULTATION	This regulation does not require consultation.
MAINTENANCE RESPONSIBILITY	The Information Technology Security Officer, Information Technology, is responsible for maintenance of this regulation.