ACCEPTABLE USE GUIDELINES

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

EMPLOYEE USE OF DISTRICT ELECTRONIC EQUIPMENT

Employees or authorized users may not remove equipment, such as desktops, laptops, and other electronic devices, from the assigned inventory location in school buildings, school offices, or classrooms unless authorization has been obtained.

For use away from work in conducting school-related business, a signed copy of an authorized Use of Equipment form shall be approved by the District instructional technology department and the employee’s direct supervisor. The form must be on file with the employee’s direct supervisor prior to the removal of the equipment from its assigned location. Equipment released to employees in such a manner may not be used for personal use and must be properly safeguarded and handled with reasonable care.

The Authorized Use of Equipment approval is for a specific piece of equipment with a unique inventory number. Review and adjustment of the equipment for offsite security may take several days.

VIOLATION OF LAW NOT PERMITTED

No user of the electronic communications system(s) may violate applicable state or federal laws, including copyright laws. Copying or using text, graphics, video and sound clips, and software may be a violation of applicable copyright laws. The user shall use care not to violate these copyright laws by use of copyrighted items. Any individual employed or contracted by the District shall determine whether use of material requires permission.

Users of the electronic communications system(s) may not publish or otherwise use personally identifiable educational records of students without permission of the student or the student’s parents unless the user complies with the Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232g.

The electronic communications system(s) shall not be used for material that is obscene or indecent, is patently offensive as measured by contemporary community standards, is sexually explicit or tends to degrade any race, religion, ethnic group, or gender.

COPYRIGHT

Copyrighted software or data may not be placed on any system connected to the District’s system(s) without permission from the holder of the copyright. Only the owner(s) or individuals the owner(s) specifically authorize may allow use of copyrighted material for use on the system(s).

SYSTEM ACCESS

Access to the District’s electronic communication system(s) will be governed as follows:

With the approval of the principal, or division/department supervisor or designee, users will be granted appropriate access to the District’s electronic communications system(s).

Any user of the District electronic communications system(s) identified as having violated District, campus, and/or division/department system acceptable use guidelines will be subject to disciplinary action consistent with District policies and regulations.

The campus principal will make the final decision regarding whether a student has violated the guidelines, subject of any right of appeal.

ACCEPTABLE USE

Access to the District's electronic communications system is a privilege, not a right. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Student access to the electronic communications system(s) is permitted unless the parent has returned the Denial of Internet Access/Electronic Publication form to the campus.

Violations of law may result in criminal prosecution as well as disciplinary action by the District.

SYSTEM COORDINATOR'S RESONSIBILITIES – Responsibilities for the system coordinator(s) (principal or division/department supervisor, or designee) will include but not be limited to the following:

1. To be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's electronic communications system(s).
2. To ensure that all users of the District's electronic communications system(s) abide by the District policies and administrative regulations regarding such use.
3. To ensure that all employees supervising students who use the District's electronic communications system(s) provide training emphasizing the appropriate uses of these resources.
4. Authorization to monitor or examine all electronic communications system(s) activities made available by University of Texas-University Charter School (UT-UCS) IT and deemed appropriate by the Superintendent or designee to ensure proper use of the electronic communications system(s).

INDIVIDUAL USER RESPONSIBILITIES - The following standards will apply to all users of the District's electronic information/communication system(s). Users who violate these standards may be subject to disciplinary action in accordance with District policies and/or administrative regulations.

SYSTEM(S) CONDUCT

1. The electronic communications system(s) may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy. Examples would be use of the electronic communications system(s) for selling commercial products and/or services or for lobbying.
2. Users may not use another person's ID or password

3. Users will maintain electronic information in accordance with established guidelines.
4. Users may not upload or download programs to or from the District’s system(s) without appropriate authorization.
5. Users may not bring unauthorized materials into the District’s electronic communications system(s).
6. Non UT-UCS equipment shall not be used on UT-UCS networks or in conjunction with District resources.
7. If a user identifies or has knowledge of a security problem on the network or any UT-UCS resource, the user must notify a system administrator.
8. The security problem should not be shown or demonstrated to other users.
9. If a user identifies or has knowledge of unsecured confidential data, the user must notify a system administrator. This includes, but is not limited to, unencrypted confidential information, unsecured transfer of confidential information, and unauthorized or inappropriate use of confidential information.
10. Exemplary behavior is expected on “virtual” field trips. When “visiting” locations on the Internet or using video conferencing or screen-sharing communication tools, users must conduct themselves as representatives of both their respective schools and the District.
11. Any District user’s traffic that traverses another network may be subject to that network’s acceptable user guidelines.

MONITORED USE

E-mail is an essential tool for communicating within and outside the University. It is important that e-mail be used in a manner that achieves its purpose without exposing UT-UCS to unnecessary technical, financial, or legal risks. The following practices are required:

Each faculty member, staff, or student using an e-mail address shall exercise prudent e-mail use in accordance with the policies, standards, and/or procedures related to Information Resources acceptable use and retention.

All e-mail is subject to logging and review.

INTELLECTUAL PROPERTY RIGHTS

VANDALISM PROHIBITED - Any attempt to harm or destroy District equipment or materials, data, of another user of the District’s electronic communications system(s), or any other agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to compromise, degrade, alter programs or settings, or disrupt system performance may be viewed as violations of District policies and administrative regulations, and possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

FORGERY PROHIBITED – Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

VIOLATION OF STANDARDS – Users who violate these standards may be subject to disciplinary action in accordance with District policy and/or legal actions.

AUTHORIZATION FOR ELECTRONIC COMMUNICATIONS SYSTEM(S) ACCESS – The District and/or systems coordinator may limit, suspend, revoke, or restore a system user's access to the District's electronic communications system(s) in accordance with District policy and/or administrative regulations regarding acceptable use.

USER LIABILITY – All communication systems resources are the property of UT-UCS. Users may be held responsible for any damage to resources caused by the user.