CROSBY INDEPENDENT SCHOOL DISTRICT

14670 FM 2100
Crosby, TX 77532
281.328.9200

Acceptable Use Policy

Employee Policies for Acceptable Use of Technology Resources

Technology resources, including Internet access, will be used to promote innovation and educational excellence consistent with the Texas Essential Knowledge and Skills and the goals of Crosby Independent School District ("Crosby ISD" or "District"). Crosby ISD believes that access to information resources and opportunities for collaboration, when used in a responsible manner, will provide educational benefit for students and employees.

The following guidelines apply to all District networks, e-mail accounts, devices connected to the District's networks, and all District-owned devices used on or off school property, whether connected to the District's network or connected through a personal data plan or other means of access.

Additionally, the District prohibits harassment through electronic means regardless of the device used, the network used, or the location of use. [See District policies DH, DIA, and FFH]

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

You are being given access to the District-provided technology resources listed below. It is important that you read the applicable District policies, administrative regulations, and this agreement form. [See policies CQ and DH, and provisions on use of electronic media in the employee handbook]

You are being given access to the following technology resources:

- A District e-mail account, including access to cloud-based (online) document storage and collaboration space (*Google Apps for Education, for instance).*
- District computer hardware, software, and printers on your school campus.
- District networks, including document storage space.
- Access to District-owned technology resources for use at home.
- District-filtered Internet access.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this policy is established to achieve the following:

1. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.

2. To establish prudent and acceptable practices regarding the use of information resources.
3. To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While CISD will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

If you are being issued a District-owned technology device that can be used off campus, you will be given additional materials addressing the proper use, care, and return of these devices.

Access to these resources is a privilege, not a right.

Ownership of Electronic Files
Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of CISD are the property of CISD.

Acceptable Use Policy

- CISD employees are assigned an individual account for access to approved CISD technology resources. Employees will not share passwords or other account information.
- CISD computer resources must be used in a manner that complies with CISD policies and State and Federal laws and regulations.
- It is against CISD policy to install or run software requiring a license on any CISD computer without a valid license.
- All software must be authorized by CISD TS prior to use. Individuals may request written approval for software/technology use through the Director of Technology Services. Unauthorized software is subject to removal upon discovery.
- Use of CISD's computing and networking infrastructure by CISD employees unrelated to their CISD positions must be limited in both time and resources and must not interfere in any way with CISD functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of CISD's networks, computer systems, applications and data resources are not permitted.
- Use of CISD computer resources for personal profit is not permitted.
- Files, images, emails or documents which may cause legal action against or embarrassment to CISD, may not be sent, received, accessed in any format (i.e. auditory, verbal or visual), downloaded or stored on CISD information resources.
- Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.
- Users must not download, install or run any programs or utilities on their systems except those authorized and installed by CISD TS and specifically designed to conduct the business of CISD. Examples of non-business related software or files include, but are not limited to: unauthorized peer-to-peer (P2P) file-sharing software, games,

unauthorized instant messengers (IM), pop email, music files, image files, freeware, and shareware. Unauthorized software may be removed upon discovery.

- Only authorized CISD staff may communicate with District students through electronic means, including social media, e-mail, and text messaging. If you are unsure whether or not you are authorized to communicate with a student through electronic means, ask your supervisor. [See DH]
- Copies of potentially sensitive or confidential District records should not be sent, viewed, or stored using an online application not approved by the District.
- Employees must not Access CISD resources to knowingly alter, damage, or delete CISD property or information, or to breach any other electronic equipment, network, or electronic communications system in violation of the law or CISD policy.
- CISD employees must not disable or attempt to disable or bypass any Internet filtering device.
- CISD employees must not encrypt communications to avoid security review.
- CISD employees must not send, post, or possess materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including material that constitutes prohibited harassment and "sexting."
- CISD employees must not use inappropriate language such as cursing, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- CISD employees must 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.

Incidental Use

As a convenience to CISD user community, incidental use of information resources may be permitted. The following restrictions apply:

- Incidental use must not interfere with the normal performance of an employee's work duties.
- Storage of personal email messages, voice messages, files and documents within CISD's information resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on CISD information resources are owned by CISD, may be subject to open records requests, and may be accessed in accordance with this policy.

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

Reporting Violations

- CISD employees must immediately report any known violation of CISD's applicable policies, Information Security Policy, or Acceptable Use Policy to the Technology Services Director.
- CISD employees must report requests for personally identifiable information, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal to the Technology Services Director.

Return of Technology Resources and Records

- Upon leaving employment, or upon request from the Superintendent, CISD employees must return any District-owned equipment or resources in their possession.
- CISD employees must also return any records, written or electronic, to the District for records retention if they have reason to believe they are retaining the sole copy of a record subject to records retention requirements. CISD employees must destroy (delete or shred) any other confidential records remaining in their possession.

Print Name:_____

Signature: _____

Campus:_____

Date: _____