

# **EMPLOYMENT EMPLOYEE STANDARDS OF CONDUCT COMPUTER ACCEPTABLE USE POLICY WEB PUBLISHING**

---

**DDDA**

## **1. INTRODUCTION**

The Tintic School District has electronic information resources available to qualifying students and teachers in our district. These resources include access to creating web pages. The District's Goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication.

## **2. WHO MAY AUTHOR WEB PAGES**

- A. Tintic Web pages can only be created by faculty members employed by Tintic Schools and their students. Individual Schools may reserve the right to implement further restrictions regarding who may author web pages.
- B. Network administrators will monitor these materials to ensure compliance with implementation standards. The content of student and faculty materials is constrained by the following restrictions:
  - 1. Schools may not publish information about students (even their names) without a signed release from the student's legal guardian(s).
  - 2. Schools may not publish information about staff (other than names, department or school, and work phone number) without a signed release from said staff.
  - 3. Individuals in pictures, movies or sound recordings may be identified only by initials (e.g. JQP for John Q. Public). Absolutely no first or last names may appear in reference to individuals in any image, movie, or sound recording without a signed release from the individual's legal guardian(s).

## **3. HOW THIS APPLIES TO WEB PAGES**

- A. Remember that anything you put on your web page is accessible to anyone in the world.
- B. Do not publish staff pictures, email addresses, home addresses or phone numbers without written permission.
- C. Do not publish student names, pictures, email addresses, or other information without written permission from their legal guardian.
- D. If you are going to allow students to publish their own web pages, or if you create web pages about your students, that will include any sort of information about the student, you must have a signed release from the legal guardian.
- E. If you create any sort of database that is accessible from the web, you must design it so that it can't be used to check whether or not a student attends a specific school. For

example, the SIS system that allows parents or students to check their grades over the World Wide Web, will require the user to enter a name and password.

#### **4. GUIDELINES AND PROVISIONS**

- A. The use of your account must be in support of education and/or research. You must attend an Internet orientation session before your account will be activated. This orientation session includes District sponsored Internet training.
- B. Transmission of any material in violation of any U.S. or Utah state regulation or statute is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene materials, anarchist\* or terrorist\* information, or material protected by trade secret.
- C. Vandalism is not permitted and will be strictly disciplined. Vandalism is defined as any attempt to harm or destroy data of another user or of another agency or network that is connected to the Internet or Intranet (District internal network). Vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses, logic bombs, ASCII mail bombs, Trojan horse programs, or any software utilized to scan the network for passwords or confidential information.
- D. Utilization of the Internet for commercial use, financial gain, personal business, product advertisement, or political lobbying activities, including lobbying for student body office, is not permitted.
- E. Attempts to tamper with another persons data or to gain unauthorized access to data on the Internet is not permitted.
- F. Use web pages to support illegal activities, as defined by local, state or federal law, is prohibited.
- G. The reconfiguration or modification of hardware, software, or network components is strictly prohibited unless given explicit verbal authorization by the network administrator.
- H. Under no circumstances shall any web page stored on or accessed from the Tintic Schools Web Server be used for obscene purposes such as the receipt, storage, or distribution of profanity or other offensive language and sexually explicit materials including nudity and other graphic or textual depiction's of sexually explicit activities. Neither shall any such page contain active links to such material. All pages on this site must meet the standards of decency of the schools and the community.
- I. Users may not maintain or retain web pages upon leaving the District.
- J. Do not present copyrighted material on your pages without permission. It is the policy of Tintic Schools that all faculty and staff must comply with state and federal copyright laws. Copyright violations related to copying printed materials, audio and video

recordings, and computer programs and databases, create potential legal liability for the Tintic School District and the individuals involved, and will not be permitted.

- K. Tintic School District cannot provide resources to host non - Tintic Schools material. The web page may contain links to remote sites, but it is not incumbent upon Tintic Schools to provide personnel time or storage space to host or manage such material. If you are using school equipment, please be sure that their use is tied firmly to the mission of Tintic School District.

## **5. RETURN TO HOME PAGE**

- A. Each page that is linked from the home page should include a "return to Tintic District home page" icon or hypertext string. Each page on the Tintic School web site should include an appropriate "return to" feature to allow for easy navigation.
  - B. Internet access in Tintic School District is a privilege and not a right. Violating any of the guidelines or prohibitions listed previously can result in restricted network access, losing all network access privileges, and/or institution of disciplinary or legal action which may include criminal prosecution under appropriate local, state, and federal laws. The systems administrator will close an account and/or restrict network access if necessary. An administrator or faculty member has the right to request, for cause, that the systems administrator deny, revoke, or suspend specific user access or account.
  - C. The Internet account holder is held responsible for his/her actions and activity within his/her account. Unacceptable uses of the network will result in the suspension or revoking of these privileges.
-