Dublin Unified School District
Technology Acceptable Use Policy and procedures
2015-2016

Dublin Unified School District ()"District") provides employees and students a variety of technology and network resources for the purpose of conducting school business. This includes any instructional and educational activities and services provided in or outside the classroom, career development, and limited high-quality self-discovery activities for students. The District also provides systems and services needed to operate and manage the District's business. This document contains the policies, procedures and acceptable use practices for users of the District's technology, which includes, by way of illustration and not limitation:

1. Electronic Communications (E-Communications):

   Any transfer of signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, received, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by the Network (defined below).

2. Electronic Communications Resources (ECRs):

   Telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that support electronic communications.

   Electronic Communications Resources include, by way of example, and not limitation: flash drives, handheld communications devices, cellular telephones, pagers, fax machines, lap top computers, net books, televisions, wireless routers, blue tooth technology, and computer monitors.

3. District Email Account:

   Any email address that is issued by the District, the Superintendent, or an authorized designee to an employee of the District, and/or others affiliated with the District, including those in program, contract, or license relationships with the District.

4. District Email Systems:

   District resources that are used to support email services and email communications including, by way of illustration and not limitation, email addresses, email software, and/or any devices for email storage. The above referenced items are collectively referred to as the "District Technology".

The Dublin Unified School District electronic network ("Network") has not been established as a public access service or a public forum. The District has the right to place reasonable restriction son material that is accessed or posted throughout the Network.

All users must sign and honor the Acceptable Use Agreement card. The District is not responsible for the actions of all users who violate this Policy. Access is a privilege –not a right.

The District reserves the right to monitor all activity on this Network. Users shall have no expectation of privacy regarding their use of the Network. All users are responsible for any damage that is caused by their inappropriate use of the Network and related components and equipment.

All users are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school and business activities, as well as the law, in the use of District Network.

All instructional personnel are expected to comply with all aspects of this Policy and provide sufficient supervision of students to ensure students' compliance.

Warning: All Technology services and systems, including the use of the Network, are to be used solely for purposes compatible with executing the District's educational and administrative business. The District reserves and shall have the right to monitor all aspects of the District Technology system, including user information, data, communications, and e-mails.

System Security

All users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them.

All users must immediately notify someone in authority (teacher or supervisor) if they have identified a possible security problem. Users will not attempt to gain unauthorized access to any portion of the District Network, including web sites blocked by District policy, another person's account, another person's folders or files, or using sniffing or remote access technology to monitor any aspect of the Network.

General Unacceptable Behaviour

While utilizing any portion of the District Network, or any District Technology, prohibited behaviors include, by way of illustration and not limitation, the following:

- transmitting of any material in violation of any federal or state law
- transmitting of any information that violates or infringes upon the rights of any other person
- transmitting of any defamatory, inappropriate, abusive, inflammatory, obscene, profane, pornographic, threatening, racially offensive, or illegal material. Do not use language that would not be appropriate in an educational setting
- transmitting of any information that encourages the use of controlled substances or the use of the Network for the purpose of inciting crime
- transmitting of any material that violates copyright laws, e.g. illegal downloading, reproduction and distribution of pirated or unlicensed copyrighted computer programs, music, or movie files
- transmitting of any vandalism, unauthorized access, 'Hacking", or tampering with hardware or software, including introducing "viruses" or pirated software (California Penal Code Section 502)
- posting information that, if acted upon, could cause damage or danger of disruption
- engaging in personal attacks, including prejudicial or discriminatory attacks (cyber-bullying)
- harassing another person. (Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages – they must stop.)
- knowingly or recklessly posting false or defamatory information about a person or organization.
- using criminal speech or speech in the course of committing a crime such as threats to the President of the United States, instruction son breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- abusing Network resources such as sending chain letters or "spamming". Students are limited to five (5) recipients per email.
- displaying, accessing or sending offensive messages or pictures.
- using the District Network for commercial purposes (i.e. offering, providing, or purchasing products or services through this
- using the District Network for political lobbying
- using any non-approved wired or wireless network (including third party internet services providers) with equipment brought from home
- attempting to access District systems (e.g. student information systems or business systems) without prior written approval by the employee's immediate supervisor and the District Technology Department
- using the Network and computer related devices are not to be used for non-educational and/or non-productive entertainment (i.e. gaming, social networking, gambling, random Internet surfing, etc.) Promoting unethical practices or any activity prohibited by law or District policy or regulation
- uploading, downloading, creating, or receiving computer viruses and/or other programs that might cause harm to the District Network
- violating other existing District or school policies and/or guidelines

- urging the passage or defeat of any ballot measure or candidate, including any candidate for election to the Governing Board (California Education Code section 7054)
- soliciting or receiving any political funds or contributions to promote the passage or defeat of a ballot measure that would affect the rate of pay, hours or work, retirement, civil service or other working conditions (California Education Code section 7056)
- interfering, or attempting to interfere with the ability of other users to send or receive e-communications
- reading, deleting, copying or modifying other users' mail unless expressly authorized by law, existing District policy, the Superintendent or other authorized designee
- using personal email addresses for District purposes
- using District ECRs, District Email Systems, and/or personal ECRs in use on District Time for any commercial or political purpose. District Time is any time a District employee is required to perform work for the District, actually performs work for the District, or is on District premises in the presence of students while school proceedings and/or activities are occurring. School proceedings include, by way of illustration and not limitation, all school-sponsored educational, extracurricular, recreational, and disciplinary activities.

Responsibility

Users are solely responsible for maintaining the confidentiality of any username and password and shall not request or use another's password. By accessing District resources and data through the use of a username and password, the user agrees to maintain the confidentiality of the username and password. Staff at the Information Technology Department should be informed of any breaches to this procedure.

Violations of this Acceptable Use Agreement

Violations of this Policy may result in loss of access as well as other disciplinary or legal action. Any violation of this Policy by a user shall be subject to the consequences as indicated within this Policy, as well as other appropriate discipline, which includes by way of illustration and not limitation:

- use of District network only under direct supervision
- suspension and/or revocation of network and computer privileges
- appropriate District disciplinary action up to and including dismissal (employee)
- appropriate District disciplinary action up to and including suspension or expulsion (student)
- legal action, prosecution or civil liabilities by authorizes
- possible fines and restitution

Due Process

The District's authorized representatives will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the District Network. Disciplinary actions will be tailored to meet specific concerns related to the violation.

Technology Hardware

Hardware and peripherals are provided for educational and school business purposes. All users are not permitted to relocate hardware (except for portable devices), install peripherals, or modify settings to equipment without the written consent of the Technology Department.

File Storage

File storage is for District business and educational related information only. Users are responsible for any files ore documents in their account. Administrators can easily gain access and read files. Do not transfer or copy any files on or off the Network Internet, or within the system. There is no public domain or shareware at the District. ALL files are to be considered copyrighted material. Copying is against the law. For example, files that should not be copied include: applications, programs, executables, zip files, movie and music files (QuickTime, MP3, etc.) etc. Students may not use any storage devices including flash drives, floppy disks or other portable and exte3rnal equipment to upload or download files.

Documents or files may be legally copied if

- they are authored by the user
- written notification from the Network administrator is given
- they can be used as part of a school assignment and/or other District projects. However, photographs and other images require large amounts of storage space and therefore will have strict limits and will be closely monitored.

Files stored on the Network are treated in the same manner as other business records. Routine maintenance and monitoring of the District Network by authorized personnel may lead to discovery that an employee has violated this Policy or the law. All users should have no expectation that files stored on District servers are private.

Users may not access or store harmful, obscene or other inappropriate materials on the Network. The District reserves the right to limit the content of information accessed or stored on the technology system for legitimate pedagogical purposes.

Printing

Printers are to be used for educatio0nal purposes and school business only. It is extremely important to use a cost-effective approach to printing to avoid waste. Fees may be required at some school sites. When printing, please follow steps below:

- Preview the document before printing.
- Print only the portion of the document needed.
- Print 2-sided (if applicable).
- User color (if applicable) only when necessary.
- Verify the printer to be used to avoid printing to unknown printers.

The particular consequences for violations of this Policy shall be determined by authorized District personnel. The Superintendent or designee and the Board shall determine when disciplinary action and/or legal action or actions by the authorities are the appropriate course of action. The Penal Code, Education Code and District policies will be adhered to when deciding disciplinary action.

E-Mail

All users may be proceed with District e-mail accounts for specific District business and school activities upon the request of school administrators or Human Resources to the District Information Technology Department.

Users of electronic mail systems should not consider electronic communications to be either private or secure; such communications are subject to subpoena. Messages relating to or in support of illegal activities must be reported to appropriate authorities.

Infinite Campus Portal

Parents and students can access a variety of student information via the Campus Portal. Parents and legal guardians can apply to the District for online access to their student's attendance, schedule, grades and additional information, as available. Students will also have access to the same information with their parent's permission.

Internet vs. Intranet

If parents do not want their student to have access to the Internet or world-wide-web (www) during school, the District can provide limited programs on the Network through our Intranet (internal network system) in which the public cannot access. The Intranet is web-based network access that is only available to staff and/or students. Information and programs on the Intranet is not available to the public.

Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District Network and/or District Technology will be error-free or without defect. The District will not be responsible for any damage suffered, including but not limited to, loss of data or interruption of service.

The District is not responsible for the accuracy or quality of the information obtained through or stored on the Network. The District will not be responsible for financial obligations arising through the unauthorized use of the Network.

The particular consequences for violations of this Policy shall be determined by authorized District personnel. The Superintendent or designee and the Board shall determine when disciplinary action and/or legal action or actions by the authorities are the appropriate course of action. The Penal Code, Education Code, and District policies will be adhered to when deciding disciplinary action.

E-Mail

All users may be provided with District e-mail accounts for specific District business and school activities upon the request of school administrators or Human Resources to the District Information Technology Department.

Users of electronic mail systems should not consider electronic communications to be either private or secure; such communications are subject to subpoena. Messages relating to or in support of illegal activities must be reported to appropriate authorities.

Infinite Campus Portal

Parents and students can access a variety of student information via the Campus Portal. Parents and legal guardians can apply to the District for online access to their student's attendance, schedule, grades, and additional information, as available. Students will also have access to the same information with their parent's permission.

Internet vs. Intranet

If parents do not want their student to have access to the Internet or world-wide-web (www) during school, the District can provide limited programs on the Network through our Intranet (internal network system) in which the public cannot access. The Intranet is web-based network access that is only available to staff and/or students. Information and programs on the Intranet is not available to the public.

Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District Network and/or District Technology will be error-free or without defect. The District will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service.

The District is not responsible for the accuracy or quality of the information obtained through or stored on the Network. The District will not be responsible for financial obligations arising through the unauthorized use of the Network.

Student signature	Date
Printed name	
Guardian signature	Date
Printed name	