556 Employee Acceptable Use of Information Technology Regulations:

"User" shall mean all persons who are granted access to the Belen Consolidated Schools' computer resources including the BCS student management system.

"Computer Resources" shall mean all computer hardware, software, communication devices, facilities, equipment, networks, Internet use, passwords, licensing and attendant policies, manuals and guides.

"Devices" shall mean all mobile technology devices, to include but not limited to ipods, ipads, cell phones, laptops, palm pilots, document readers, in focus projectors, as well as desktop equipment purchased with district funds, whether operational, grant, or federal.

No expectation of privacy. The computers and computer accounts given to Users are to assist them in enhancing student academic achievement and job performance. Users do not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to BCS and may be used only for education program purposes.

Waiver of privacy rights. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or mobile device or through the Internet or any other computer network. Users consent to allowing BCS personnel access to review all materials users create, store, send, or receive on the computer or mobile device or through the Internet or any other computer network. Users understand that BCS may use human or automated means to monitor use of its computer resources.

Access to or Creation of inappropriate or unlawful materials. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, threatening or potentially violent, defamatory, racially offensive, proselytizing, inappropriate or otherwise unlawful, or in violation of School Board policy may not be created, accessed or sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

Prohibited uses. Without prior written permission from the District's Superintendent or designee, computer resources may not be used for dissemination or storage of commercial or personal advertisements, promotion, destructive programs (including but not limited to self-replicating codes or viruses), political or religious materials, or any use which is unauthorized or in violation of School Board policy.

Waste of computer resources. Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion or detriment of others. These acts include, but are not limited to, sending or forwarding mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, sending or forwarding jokes, engaging in online chat groups, printing multiple copies or documents, or otherwise creating unnecessary network traffic.

Misuse of Software. Without prior written authorization from the BCS Technology Coordinator, Users may not do any of the following: (1) copy software for use on their home computers; (2) provide copies of software to any third person; (3) install software on any School District workstations, servers, or devices; (4) download any software or run executable files from the Internet, email, or other online service to any BCS workstations, servers, or devices; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse-engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to their site administrator.

Communication trade secrets. Unless expressly authorized by the BCS Superintendent or designee, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of BCS is strictly prohibited.

Responsibility for passwords. Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. **No User may access the computer system with another User's password or account.**

Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. BCS has global passwords that permit it access to all material stored on its computer system, regardless of whether or not material has been encoded with a particular User's password.

Accessing other user's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. A Users ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other users or BCS operational systems by unnecessarily reviewing their files and e-mail without authority.

Accessing other computers and networks. A User's ability to connect to other computers/systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

Computer security. Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of BCS Computer Resources including the BCS student management system. This duty includes taking reasonable precautions to prevent intruders from accessing the BCS network via Internet connections or by leaving systems on and logged into the network without authorization and to prevent the introduction and spread of viruses.

Each User agrees that he or she has a greater responsibility to be mindful of FERPA issues and understands the consequences of discussing confidential information with unauthorized individuals.

CIPA. **ALL** Users of the Internet must comply with the Children's Internet Protection Act (CIPA), 47 U.S. C254 **Internet Safety** Policy. Access by minors to inappropriate matter on the Internet and World Wide Web is prohibited on BCS devices. Using chat rooms and other forms of direct electronic communications is prohibited on the BCS network. Unauthorized access including "hacking" and other unlawful activities by minors online is prohibited on the BCS network. Unauthorized disclosure, use, and dissemination of personal information regarding minors is prohibited by BCS. Measures designed to restrict minor's access to materials harmful to minors are in place at BCS.

MISUSE OF HARDWARE. Users may not deliberately remove, turn off, or otherwise circumvent the existing security profiles set up on district devices. The BCS approved filtering device is loaded onto all BCS computer devices, including mobile devices such as ipads, ipods, cell phones, and palm pilots. Users may not download other browsers or programs onto district devices.

*Virus detection***.** Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the BCS network. To that end, all material received on floppy disk, CD, flash/zip/thumb drive or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to BCS **MUST** be scanned for viruses and other destructive programs before being placed onto the system or network. Users should understand that their home computers and laptops may contain viruses. All disks and other media transferred from these computers to the BCS network **MUST** be scanned for viruses.

Use of encryption software. Users may not install or use encryption software on any of the BCS computers or devices without first obtaining written permissions from the District Technology Coordinator or designee. Users may not use passwords or encryption passwords that have not been provided by the District Technology Coordinator or designee.

Export restrictions. The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in anyway outside the United States without the prior written authorization from the District Technology Coordinator Director.

Compliance with applicable laws and licenses. In their use of computer resources, Users must comply with all software licenses, copyrights, all other state, federal, and international laws governing intellectual property and online activities.

Accessing District Student Management System. Users authorized to externally access the district's student management system are responsible for ensuring that unauthorized person(s) do not gain access to the district's student management system information by safeguarding passwords, safeguarding the environment used to gain access, and maintaining confidentiality of student information.

Users agree that they are responsible for the security, confidentiality and integrity of the school-related work done beyond district boundaries.

Users are responsible for safeguarding their passwords for access to the district's student management system. User passwords for the district's student management system must be unique and not be used for anything else. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the district's student management system with another User's password or account.

Other policies applicable. In their use of Technology Resources, Users must observe and comply with all other policies and guidelines of BCS.

***User Responsibility*. User is responsible for backing up all individual work done using District Technology resources.**

No additional rights. This Policy is not intended to, and does not grant, Users any contractual rights.

Violation of Policy. Violation of this policy will result in loss of access to network and/or district resources, and possible legal and disciplinary action.

Belen Consolidated Schools

Employee Acceptable Use of Information Technology Agreement

2017-2018 SY

Please read the attached document carefully before signing. Return the signed form to your site administrator.

Belen Consolidated Schools, BCS, has a network of computers with Internet access. Use of the network is a privilege dependent on agreement to and compliance with the employee Acceptable Use of Information Technology agreement. The use of any BCS network resource constitutes use whether or not the user has a network account.

I understand and will abide by the Belen Consolidated School District Personnel Policy 556 regulations. Should I commit any violation, school disciplinary and/or appropriate legal action may be taken.

User Name (Please print) _____ Date _____

User Signature _____ Date _____

Work Site (school/district department) _____

SEND ORIGINAL of this page to Human Resources.

KEEP COPY of this page at site or with department administrator.