~~USDB~~ Employee Acceptable Use Policy

Draft 1

~~Reviewed/Revised: August 2019~~	~~Effective Date: August 1, 2015~~
Effective Date:	
Authorized By: ~~Joel Coleman, Superintendent~~ Utah State Board of Education	

1. **PURPOSE**
   1.1. This policy intends to (1) set forth the terms and conditions under which Utah Schools for the Deaf and the Blind ("USDB") Users may access and use USDB Network and Computer Resources; (2) state the requirements that shall govern the operation and management of all information technology used, operated and/or maintained by USDB; and (3) ensure the USDB's information technology and information assets are managed so as to maximize their efficient and secure use.

2. **APPLICABILITY**
   2.1. This policy applies to all employees, officers, temporary employees, interns, vendors, consultants, contractors and authorized agents and volunteers working under the supervision of a school supervisor, who use USDB Computer Resources and/or access the USDB Network ("Users"). ~~Students are subject to and must comply with USDB's Policy on Student Use of the USDB Network and Computer Resources~~. Personal electronic devices are subject to this policy when such devices are connected to the USDB Network or Computer Resources.
   2.2. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges may be terminated, access to the School's technology resources may be revoked or denied, and appropriate disciplinary action shall be applied.

2.3. **Violations may result in disciplinary action up to and including ~~suspension for students~~ or termination ~~for employees~~. When applicable, law enforcement agencies may be involved.**

2.4. Users who leave USDB for any reason ~~during the school year~~ must surrender all electronic devices, data and other technology-related resources. Failure to return an electronic device will result in a theft report being filed with the local Police Department.

3. **DEFINITIONS**

3.1. **Computer Resources** refers to the full scope of an organization's Information Technology (IT) assets used to conduct business, regardless of location or ownership. This includes computing devices, infrastructure (i.e., networks, data storage, virtual environments, etc.), communication and output devices, and peripherals or accessories. ~~all computers and information technology, whether stationary or portable, used to conduct the day-to-day business of USDB, including but not limited to all related peripherals, components, disk space, storage devices, system memory, servers, telecommunication devices and output devices such as telephones, hand held devices, printers, scanners, facsimile machines and copiers whether owned or leased by USDB.~~

3.2. **Collaboration Systems** refers to the comprehensive suite of hardware and software tools designed to facilitate both real-time (synchronos) and delayed (asynchronous) communication and teamwork across the organization. These systems that support remote and digital workflows leverage multiple devices and channels, including but not limited to: unified communications platforms, real-time messaging, project and content management, scheduling and conferencing, and knowledge sharing. This definition includes all platforms used to connect individuals and teams for shared work.~~ systems which support synchronous and asynchronous communication through a variety of devices, tools and channels. Examples of collaboration systems include, but are not limited to: calendaring, message/conference boards, blogs, text chat/instant messaging, video conferencing, websites and podcasting~~.

3.3. **Network Infrastructure ~~USDB Network~~** refers to the entire

electronic framework used for transmitting, storing, and accessing all data and applications for the organization. This includes but is not limited to: connectivity, data systems, and internal resources whether USDB owned or leased. ~~infrastructure used to transmit, store and review data over an electronic medium and includes, but is not limited to, the USDB E-mail system(s), collaboration systems, databases, internet service, the USDB intranet system, whether the system is owned or contracted~~.

3.4. **Department/School Management** refers to the supervisor, manager, director, officer, Principal, or other USDB employee designated by his/her department or office or school to implement Policy compliance requirements.

3.5. **ITS** refers to the USDB Information Technology Services Department.

4. **DUTIES**

4.1. **ITS Duties:** ITS is responsible for designing, establishing and maintaining the USDB Network and Computer Resources and for assisting Users in all USDB departments, offices, and schools in implementing and maintaining electronic information management and security practices at their respective locations. ITS shall establish and issue procedures, standards and guidelines (collectively referred to as ITS Guidelines) as necessary to implement the requirements of this Policy or to specify the terms of use for a particular USDB Network system or Computer Resource.

4.2. **Department/School Management Duties:** Department/School Management are responsible for designating Users authorized to use the USDB Network and Computer Resources and providing for their individualized access to specific USDB Network systems based on job duties. Department/School Management shall enroll and terminate User access to USDB Network and Computer Resources in accordance with ITS Guidelines. Department/School Management will approve access to the USDB Network and Computer Resources by Users who are not USDB employees, such as consultants or contractors, only when access is required for the consultant or contractor to perform critical functions and services, and only upon the consultant's/contractor's execution of a confidentiality

agreement regarding such access and use.

5. **OWNERSHIP AND PRIVACY**

5.1. **Privacy:** Users have no expectation of privacy in their use of the USDB Network and Computer Resources.

5.2. **Monitoring and Access Rights:** The IT Department retains the unilateral right to monitor, log, inspect, search, read, and copy all data communications, and activities stored, transmitted, or processed on the Organization's network and computing resources, including but not limited to email and internet usage, to ensure policy compliance, system security, and for legal purposes. The IT Department reserves the right, without prior notice to: modify systems, deny access, and intercept or quarantine digital communications. The IT Department will determine and enforce appropriate resource use, and report any illegal activity to the proper authorities. ~~ITS has the right to access, search, read, inspect, copy, monitor, log or otherwise use data and information stored, transmitted and processed on USDB Network and Computer Resources in order to execute the requirements of this policy. USDB Network including but not limited to Internet and Email usage may be monitored and audited by Department/School Management and ITS for inappropriate activity or oversight purposes. ITS reserves the right to: (1) access and make changes to any system connected to the USDB Network and Computer Resources to address security concerns, (2) deny User access to any system to address security concerns, and (3) determine what constitutes appropriate use of these resources and to report any illegal activities. ITS may intercept and/or quarantine email messages and related resources, such as Internet mail and other messaging services for business, legal or security purposes.~~

5.3. **Manager Access:** Department/School Management may access documents, data and information generated, stored, transmitted or processed by a User on the USDB Network and Computer Resources in accordance with ITS Guidelines. A User's supervisor may also access a User's USDB Network account for business purposes, including oversight purposes, regardless of whether the User is present or absent. In all cases, the Department/School Management shall contact the Help Desk to obtain access. Supervisors shall not ask Users

to share their password for such purposes.

6. GENERAL PROVISIONS REGARDING USE

6.1. **Personal Use:**Use of USDB Network and Computer Resources is intended for Agency business, with limited personal use permitted. Such personal use must in all circumstances comply with the acceptable use and conduct provisions in this policy, and must not result in costs to USDB, cause legal action against or cause embarrassment to USDB. Such use must also be appropriate as to duration and not interfere with the User's duties and USDB's business demands.

6.2. **Unacceptable Use:** Unacceptable use of the USDB Network and Computer Resources is prohibited. Users shall not use the USDB Network or Computer Resources including access to the Internet, Intranet, Collaboration Systems or E-mail to use, upload, post, mail, display, store, or otherwise transmit in any manner any content, communication or information that, among other unacceptable uses:

6.2.1. is hateful, harassing, threatening, libelous or defamatory;

6.2.2. is deemed offensive to persons based on race, ethnic heritage, national origin, sex, sexual orientation, age, physical or mental illness or disability, marital status, religion or other characteristics that may be protected by applicable civil rights laws;

6.2.3. constitutes or furthers any criminal offense, or gives rise to civil liability, under any applicable law, including, without limitation, U.S. export control laws or U.S. patent, trademark or copyright laws;

6.2.4. constitutes use for, or in support of, any obscene or pornographic purpose including, but not limited to, the transmitting, retrieving or viewing of any profane, obscene, or sexually explicit material;

6.2.5. constitutes use for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass, threaten, or "stalk" another individual;

6.2.6. contains malware or other malicious code; ~~a virus, Trojan horse, logic bomb, worm or other harmful component or malicious code;~~

6.2.7. constitutes a chain letter, junk mail, phishing, spam or unauthorized broadcast e-mail;
6.2.8. violates the security of any computer or network or constitutes unauthorized access or attempts to circumvent any security measures;
6.2.9. obtains access to another User's USDB Network account, files or data, or modifies their files, data, or passwords, unless explicitly authorized to do so;
6.2.10. impersonates any person living or dead, organization, business, or other entity;
6.2.11. degrades the performance of the USDB Network or Computer Resources or causes a security risk;
6.2.12. deprives an authorized User of access to USDB Network or Computer Resources;
6.2.13. obtains resources or USDB Network access beyond those authorized,
6.2.14. engages in unauthorized or unlawful entry into a USDB Network system;
6.2.15. discloses confidential or proprietary information, including student record information, without authorization or without proper security measures;
6.2.16. shares USDB e-mail addresses or distribution lists for uses that violate this policy or any other USDB and/or State policy;
6.2.17. enables or constitutes gaming, wagering or gambling of any kind;
6.2.18. promotes or participates in any way in unauthorized raffles or fundraisers,
6.2.19. promotes or participates in any way in partisan political activities;
6.2.20. promotes or participates in any way in internal political or election activities related to a union or other organization representing employees;
6.2.21. engages in private business, commercial or other activities for personal financial gain;
6.2.22. distributes unauthorized information regarding other Users' passwords or security systems;
6.2.23. solicits or distributes information with the intent to cause personal harm or bodily injury;
6.2.24. transmits sensitive or confidential information without appropriate security safeguards;

6.2.25. falsifies, tampers with or makes unauthorized changes or deletions to data located on the USDB Network;
6.2.26. enters false data on to the USDB Network;
6.2.27. accesses or uses data located on a USDB Network system for personal uses;
6.2.28. promotes or participates in a relationship with a student or which is not related to academics or school-sponsored extracurricular activities, unless authorized in advance in writing by the Superintendent and the student's parent/guardian;
6.2.29. installs, downloads or uses unauthorized or unlicensed software or third-party system;
6.2.30. violates the terms of use specified for a particular Computer Resource or USDB Network System;
6.2.31. violates federal or state law or any USDB and/or State rules, policies, standards or guidelines regarding the protection of employee or student privacy or the confidentiality of employee or student records; or
6.2.32. violates any express prohibition noted in this policy or any other USDB policy.

7. **SECURITY**

7.1. **Passwords:** Passwords and PIN numbers should be kept confidential; do not allow other individuals to use your device or password. It is not appropriate for a supervisor to require a subordinate to share their password. ~~Because secure passwords are so vital to system security, users are required to change passwords a minimum of every 90 days.~~ All electronic devices capable of being password or pin secured must have security enabled.

7.2. **Unattended devices:** Electronic devices should not be left unattended without taking measures to prevent intrusion or unauthorized access. When not personally attended, devices should be locked using their built-in security, or turned off.

7.3. **Physical security:** Electronic devices should be stored in a securely locked location when not in use.

7.4. **Filtering and Blocking:** As required by law, USDB ITS uses filtering technology to screen internet sites for offensive material and prohibit access, to the extent possible, to objectionable, offensive or unsuitable content found on the internet. In addition to the use of filtering technology, ITS may

also block access to certain websites when required by law, when their use may interfere with the optimal functioning, or when among other things, the website may compromise the security of the USDB Network or Computer Resources. ITS shall establish standards and procedures by which individual websites may be authorized for blocking or unblocking of access from the USDB Network. All blocking and unblocking decisions will be made by ITS in compliance with applicable laws and the requirements of this policy.

7.5. **Portable Devices:** All Computer Resources that are considered portable devices are subject to additional security requirements as set out in the ITS guidelines. Users shall abide by all requirements established by ITS for such portable devices, including but not limited to those related to laptops, cell phones, smart phones, USB memory sticks, and portable hard drives. Users are prohibited from housing Personally Identifiable Information (PII) on a portable device without the prior approval of ITS.

7.6. **Email:** All staff must exercise extreme caution to ensure that email messages containing confidential student or staff information adhere to privacy laws. Staff must verify that emails are sent only to intended, authorized recipients and follow all USDB standards and guidelines for classifying, handling, and securing confidential data, including the use of required encryption when transmitting sensitive information. ~~Users must exercise due care to ensure that e-mail messages containing confidential information conform to the confidential transmission requirements noted herein and are transmitted only to their intended recipients. Users are prohibited from transmitting Social Security Number information via e-mail without the prior written approval of ITS. Users shall abide by ITS-issued standards and guidelines on the classification, handling and email transmission of confidential information, including applicable encryption requirements.~~

8. SOFTWARE

8.1. **Software Licensing and Software Copying:** Every effort is made to stay in compliance with software license agreements by having sufficient licenses for every user or by restricting access to a limited number of licenses. Copies of software licensed by our agency should never be copied for use

elsewhere unless specifically permitted by authorized IT staff.

8.2. **Personal Software:** In the event that users have purchased software licenses for personal use on home computers or electronic device, users are not authorized to install copies of that software on agency owned computers. As a rule, public domain software and shareware should not be installed on agency machines without first obtaining permission from a system administrator.

9. REPORTING

9.1. Users shall immediately report to the USDB Help Desk and Department/School Management any actual or suspected:

9.1.1. security violations or breaches, including, but not limited to:

9.1.2. improper transmission of confidential information;

9.1.3. compromised passwords or access codes

9.1.4. receipt of messages containing suspected malicious ~~virus~~ content;

9.1.5. theft or loss of Computer Resources including portable devices

9.1.6. unacceptable use of the USDB Network or Computer Resources; and

9.1.7. any other violation of this Policy.

9.2. Receipt of inappropriate spam or suspicious electronic messages, including suspected phishing messages, should be reported immediately to USDB IT using established reporting procedures (helpdesk@usdb.org, Ext 4787.) User access privileges may be suspended at any time if ITS determines that a security threat exists.

10. VIOLATIONS AND ENFORCEMENT OF THIS POLICY

10.1. Employees who fail to abide by this policy are subject to discipline in accordance with USDB's Employee Discipline and Due Process Policy with corrective action ranging from suspension or permanent revocation of USDB Network access privileges to termination of employment. Violations of certain provisions in this policy may also subject a User to civil and criminal liability according to applicable federal and state laws. Any USDB contractor, consultant, volunteer or other business partner who violates this policy may have their system access privileges suspended and may further be subject to contract

termination or any other remedy or action deemed appropriate by USDB.

I agree to adhere to this policy in its entirety.

_____

Name (please print)

_____

Signature Date