Rescue Union School District
Exhibit

E 4040
Personnel

Employee Responsible Use of Technology

RESPONSIBLE USE AGREEMENT FOR STAFF MEMBERS

Rescue Union School District (RUSD) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st Century technology and communication skills and the district continues to invest in making technology an integral part of the district's core mission of educating every child in addition to making these resources available to all staff in the business and administrative functions of the school district. To that end, we provide access to technologies for student and staff use. This **RESPONSIBLE USE POLICY for Staff** outlines the guidelines and behaviors that staff is expected to follow when using District technologies to perform their responsibilities and when using personally-owned devices on the District network. Responsibility for use of technology and electronic information that does not comply with the Acceptable Use Agreement lies with the individual employee.

RESPONSIBLE USE means that RUSD students and employees will benefit educationally from these resources while remaining within the bounds of safe, legal and responsible use. The use of RUSD technological resources, including access to the Internet, is a privilege, not a right. Individual users of District technology are responsible for their behavior and communications when using those resources. Accordingly, the District establishes this policy to govern employee use of District technological resources. This policy applies regardless of whether such use occurs on or off District property when utilizing District technological resources.

Before using District technologies, the network and services, RUSD staff shall sign the District's Responsible Use Policy indicating that the RUSD staff member understands and agrees to abide by specified user obligations and responsibilities as outlined in this agreement and in Board policy found at http://www.rescueusd.org/Technology**. Inappropriate use of these resources may result in loss of privileges as well as the suspension or revocation of access to these resources at any time and/or in disciplinary action and/or legal action, which may include the possibility of termination and/or referral to legal authorities.**

USAGE POLICIES AND TECHNOLOGY TOOLS:

All technologies provided by the district are intended for education purposes as it relates to the teaching, learning, business and administrative functions of the District.

RUSD USERS ARE RESPONSIBLE TO:

- Follow the specifics and intent of this document
- Use good judgment and responsible professional judgment
- Be safe, appropriate, careful and kind
- Be respectful of the District's technological protection measures
- Abide by the generally accepted rules of network etiquette

- Follow RUSD Board Policy and Administrative Regulations including but not limited to:
    - BP 4040 and AR 4040 – Employee Use of Technology
    - BP 6163.4 and AR 6163.4 – Student Use of Technology
    - BP 5131and AR 5131 – Student Conduct (includes use of cell phones by students)
    - BP 1113 and AR 1113 – Web Sites

Staff members are responsible for the proper use of all equipment in their office space or classroom. The policies outlined in this document are intended to cover all available technologies. This also includes Personal Electronic Devices (PEDs) when connecting to the RUSD network as allowed through this policy and Board Policy.

NETWORK, E-MAIL AND INTERNET USE

RUSD USERS ARE RESPONSIBLE TO:

- Utilize work email predominantly for work related purposes
- ***Communicate with the same appropriate, safe, mindful, courteous conduct online as offline***
- Delete emails or links from unknown or un-trusted sources
- Use content from the Internet, in accordance with copyright and plagiarism laws
- Understand that the District network may not be used by any device (including personal devices) for any illegal activity, malicious attacks, hacking, or peer-to-peer file sharing (i.e., BitTorrent, Gnutella or Kazaa.) on this network or any other
- Understand that messages, information or graphics sent, viewed, downloaded, provided or intentionally received which include/suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, listings or otherwise objectionable material shall result in consequences and/or disciplinary action

STUDENT SAFETY AND SECURITY OF STUDENT DATA

RUSD USERS ARE RESPONSIBLE TO:

- ***Supervise student computer use and student Internet use, and to take appropriate action if student computer misuse is discovered per Board policy***
- Understand that the District provides a software-based filtering solution to protect students and to monitor all Internet usage
- Understand that the District cannot guarantee that students and staff will not gain access to inappropriate material
- Follow Board Policy 1113 and Administrative Regulation 1113, Web Sites if posting images of students
- Instruct students on Internet safety and the appropriate and ethical use of information technology in the classroom including copyright, plagiarism and fair use using District adopted curriculum appropriate to their grade level
- Put into place rules and procedures that guide student use and that safeguards technology equipment against damage or misuse
- Only access student data if the District has given the user permission to do so with their individual login
- Protect and secure all data from students, parents/guardians, other unauthorized staff and volunteers including data in the District's student information system and any other database containing student information or data.

NETWORK USAGE, SECURITY AND STAFF SAFETY

RUSD USERS ARE RESPONSIBLE TO:

- Use the individually District assigned login account to access the RUSD network, databases, workstations, or other technological resources
- **Keep individual usernames and passwords confidential and understand it is a violation of this policy to share that information with others**
- Monitor and maintain responsible files sizes or amounts of storage on the assigned work computer(s), the network and in email. Employees who take up large amounts of space with personal files (including music and pictures) will be asked to remove the resources from the network
- Take reasonable safeguards against the transmission of security threats over the school network
- Notify the District Technology Department if a computer or mobile device might be infected with a virus or otherwise be compromised
- Understand that users identified as a security risk for having a history of discipline and/or responsible use problems with other computer systems will be denied access to RUSD workstations and the Internet by the Rescue Union School District

SOCIAL MEDIA GUIDELINES

Staff is expected to maintain professional conduct at all times when online. Using social media has the capacity to cause irreparable damage to you personally and/or professionally if something inappropriate or illegal is posted by yourself or someone you communicate with.

The following recommendations and guidelines are intended to serve as guidelines for all District personnel who elect to engage in social media, regardless of whether such online activity occurs during working or non-working time. If any employee is uncertain about how to apply these guidelines or has questions about participation in social media, they are expected to seek the guidance of a supervisor or other appropriate district administrator.

RUSD RECOMMENDS THAT STAFF WHO UTILIZE SOCIAL MEDIA:

- Decline and avoid online "friendships" with students or parents
- Understand that anyone classified as a "friend" has the ability to download and share your information with others and may also post inappropriate comments, pictures or other material that could negatively impact your professional reputation
- Understand that only District-endorsed networking platforms which have restricted access should be used to engage with students for educational purposes
- Not post any material that should not be seen by students, parents, or school administrators
- Avoid discussion or identification of students or personnel in social media

MOBILE DEVICES POLICY

RUSD USERS ARE RESPONSIBLE TO:

- ***Abide by this Responsible Use Policy when using District provided mobile devices on and off of the District network***
- Sign the Mobile Device Responsible Use Policy (MDRUP) prior to using any District issued mobile device.
- Use mobile devices with extreme care and caution
- Report any loss, damage, or malfunction to District IT staff immediately
- Understand that they may be financially accountable for any damage resulting from negligence or misuse

PERSONAL ELECTRONIC DEVICES (PEDS) PED INTRODUCTION AND DEFINITION

Personal electronic device (PED) includes, but is not exclusive of mobile phones, USB drives, MP3 players, PDAs, laptop computers, tablet computers, DVD players, and calculators.

RUSD embraces emerging digital technologies and encourages teachers and students to look for ways of using them to enhance teaching and learning. The availability and appropriate use of these resources provide opportunities that can help students develop academically, socially and physically. The technology of mobile phones and other electronic devices to facilitate the recording of sound, take photographs and video images is open to abuse that can lead to an invasion of a person's privacy. Inappropriate use can be detrimental to the teaching and learning process, is anti-social, and may be harmful to both students and staff.

PERSONAL ELECTRONIC DEVICES (PEDS)

FOR PEDS THAT CONNECT TO THE DISTRICT'S WIRELESS NETWORK, RUSD USERS ARE RESPONSIBLE TO:

- Understand that the ***RUSD Responsible Use Policy for Staff*** also applies to personally owned electronic devices when on the District network or when utilized for work purposes
- Connect PEDs to the District network via wireless Ethernet technology and not via direct Ethernet structured cabling
- Understand that the District will not be held responsible for the loss, theft or destruction of any personal electronic devices
- Understand that the District reserves the right to review suspicious activity and/or flagged files on any mobile device brought into a district or school facility
- Understand that any violation of these rules will result in the loss of the staff member's privilege to bring personal mobile devices to a district or school facility
- Use PEDs responsibly and to never abuse a person's right to privacy (for example, taking, storing and then using a digital photo/video without a person's permission)
- Run the latest virus protection software and security patches for operating systems
- Ensure the device is free of spyware, adware, worms, viruses, trojan horses, and peer to peer software that could disrupt or damage the network
- Ensure the device is not running Internet or web hosting services and does not have Internet Connection Sharing services turned on

NO EXPECTATION OF PRIVACY

RUSD USERS ARE RESPONSIBLE TO UNDERSTAND THAT:

- ***No right of privacy exists in the use of RUSD technological resources***
- Understand that anyone who does not comply with the provisions of this agreement may have their user privileges cancelled and personnel action may be taken at the discretion of the District after application of due process
- Files or communications created or transmitted using District technological resources or stored on services or hard drives of individual computers will not be private
- District personnel shall monitor online activities of all users who access the Internet utilizing the District network
- District / school administrators or individuals designated by the superintendent may review files, monitor all communication and intercept e-mail messages for the safety of students, to maintain system integrity and to ensure compliance with Board policy and applicable laws and regulations
- Use of District provided mobile devices may be monitored on and off the District network at any time
- Unintentional access to inappropriate or illegal materials should be reported immediately to the staff member's immediate supervisor

CONSEQUENCES FOR IMPROPER USE:

All employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using District technological resources, employees must sign a statement indicating that they understand and will strictly comply with these requirements. Any user violating rules, applicable to state and federal laws, or posted classroom and District rules, is subject to loss of network privileges and other disciplinary actions and/or the loss of employment and benefits including possibility of denial, suspension, or revocation of the credential of a certificated employee due to misconduct. In addition, pertaining to State and Federal laws, any unauthorized access, attempted access, or use of any state computing and/or network system is a violation of Section 502 of the California Penal Code or applicable federal laws and is subject to criminal prosecution.

DISCLAIMER:

The Rescue Union School District makes no warranties of any kind, whether express or implied, and will not be held responsible for the loss of data or service resulting from delays, non-deliveries, or service interruptions sustained or incurred in connection with the use, operation, or inability to use the system. **The District recommends employees keep a separate personal backup of those items which are critical to them. Additionally, the District specifically denies any responsibility for the accuracy or quality of information obtained electronically and use of information obtained electronically is at the risk of the user. While RUSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. RUSD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.**

PLEASE RETAIN A COPY OF THIS PAGE FOR YOUR FILES

I have read and agree to the Rescue Union School District's *Responsible Use Agreement* and understand that I will be required to read and agree to follow this policy on an annual basis (in print and/or digital format):

Employee Signature	
Employee Name (print)	Date
School Site / Work Location (print)	Department or Grade:
Position Title:	Hire Date:
WHEN CREATING PASSWORDS: • *Usernames will be employee's first initial, last name (Jane Doe: jdoe)* • *Passwords must not be easy to guess such as family names, pet names, etc.* • *Password must contain at least one capital letter, one number and one special character; $, !, #, etc.* • *Password will be utilized for logging onto the computer, e-mail, and Follett as applicable to the user.*	

**This policy is CIPA (Children's Internet Protection Act) Compliant, FERPA Complaint