**ALL PERSONNEL**

# Employee Use of Technology Acceptable Use Agreement and Release of District from Liability (Employees)

The McFarland Unified School District recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs. This policy applies to and describes the responsibilities and obligations of all employees using the District's electronic information resources, including computers, electronic devices, and network, and portions of this policy also apply to an employee's personal computer and electronic devices under certain circumstances.

The McFarland Unified School District authorizes district employees to use technology owned or otherwise provided by the district necessary to fulfill the requirements of their position. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason. This document is legally binding on employees, whether or not they have signed the Acceptable Use Agreement. District supervisors are required to enforce these policies consistently and uniformly. No supervisor has the authority to override the policies unless he/she obtains the written permission of the Superintendent. Signed Acceptable Use Agreements are kept on file at McFarland Unified. Any employee who violates any provision of this Acceptable use agreement shall be considered as having acted in an individual capacity and outside the scope of employment and, as such, may be subject to disciplinary action, up to and including termination or criminal prosecution by government authorities. The following statements are provided in accordance with Board Policy 4040.

The district expects all employees to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable restrictions on sites, material, and /or information that employees may access through the system. The district makes no guarantee that the functions or services provided by or through the district will be without defect. In addition, the district is not responsible for financial obligations arising from unauthorized use of the system. Each employee who is authorized to use district technology shall sign this Acceptable Use Agreement as an indication that he/she has read and understands the agreement.

## Definitions

1. The term "electronic information resources" ("EIR") includes district computers, electronic devices, and the District's electronic network and software.
2. The term "district electronic record" means any writing containing information relating to conduct of the District's business where the writing was prepared, owned, used, or retained in electronic/digital format by the District, regardless of where or how the record may have been prepared or where the record is retained. Records containing no more than incidental references to the District are not considered district electronic records. For this purpose, "writing" means anything in an electronic/digital format including sounds, images, symbols, words, or any combination thereof, specifically including electronic mail (email) and all other forms of electronic files.

3. The term "computer" means any computer, including a laptop or notebook, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.
4. The term "district computer" means any computer owned, leased, or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by or donated to the District from another agency, company, or entity, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

5. The term "electronic device" means any device, other than a computer, capable of transmitting, receiving, or storing digital media, whether or not the electronic device is portable and whether or not it is equipped with a modem or other communication peripheral capable of digital connection. Electronic devices include but are not limited to the following:
• Telephones
• Cellphones, including "smartphones"
• Radios
• Pagers
• Digital cameras
• Personal digital assistants, including but not limited to Blackberries, Palm Pilots, and "smartphones"
• Portable storage devices, including but not limited to thumb drives and zip drives
• Portable media devices, including but not limited to iPods, iPads, other tablets (e.g., Nook, Kindle, etc.), and MP3 players
• Optical storage media such as compact discs (CDs) and digital versatile discs (DVDs)
• Printers and copiers
• Fax machines
• Portable texting devices
6. The term "district electronic device" means any electronic device owned, leased, or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by or loaned to the District from another agency.
7. The term "district electronic network" means the District's local area district-wide network and internet systems, whether hardwired or wireless, including software, email and voicemail systems, remote sites, and/or VPN connections.
8. The terms "personal computer" and "personal electronic device" mean computers and/or devices as defined in this policy that are not district computers or electronic devices, typically computers and/or devices owned by individuals including employees and visitors. Personal cell or smartphones, iPads, and similar devices are personal electronic devices, whether or not supported by a district stipend paid to the employee.

## OWNERSHIP

District EIR is district property provided to meet district needs and does not belong to employees. Use of district EIR is a privilege which the District may revoke or restrict at any time without prior notice to the employee. All district computers and district electronic devices are to be registered to the District and not to an employee. All software on district computers and district electronic devices is to be registered to the District and not to an employee, except as otherwise provided in this policy. No employee shall remove a district computer or district electronic device from district property without the prior, express authorization of the employee's supervisor.

## NO EMPLOYEE PRIVACY

Employees have no privacy whatsoever in their personal or work-related use of district EIR, or to any communications or other information contained in district EIR or that may pass through district EIR. With or without cause and with or without notice to the employee, the District retains the right to remotely monitor, physically inspect, or examine district computers, electronic devices, network, or other EIR, and any communication or information stored on or passing through district EIR, including but not limited to software, data and image files, internet use, emails, text messages, voicemail and social media.

**All** email sent and received via the district email system, including email of a personal nature, will be captured and retained in a central location for a period of time determined by the District to be appropriate. Deletion of email from computers and electronic devices will not delete captured and

retained email. The email that is captured and retained in a central location is the District's official record of the email, no matter where other copies of that email may be found.

District EIR will be inspected for software and/or virus-like programming, including commercial software applications that harvest, collect, or compromise data or information resources. Any computer or electronic device containing those elements may be disconnected, blocked, or otherwise isolated at any time and without notice in order to protect district EIR. This includes personal computers and/or electronic devices that an employee may connect, with or without proper authorization, to district EIR. Due to the commonplace presence of such software and Apps on personal computers and/or devices, their connection to district EIR without prior authorization is discouraged.

When an employee leaves employment with the District, management shall be given access to and the authority to dispose of any and all district electronic records, including the employee's computer files, email, voicemail, text messages, and any other electronic information stored on district EIR. Employees leaving their employment shall provide the District with all files and other electronic records from personal computers and devices, and employees shall not delete those items from district EIR.

Employees should be aware that, in most instances, their use of district technology (such as web searches or emails) cannot be erased or deleted. All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee on district technology does not create a reasonable expectation of privacy. I also understand that in order to comply with state and federal student privacy laws, I will not allow people who are not District employees (such as parents, volunteers, or students) to use or access my District issued computing device since confidential or protected student information or sensitive District email communications may be stored or accessed from there.

Both student and employee records are protected by various state and federal laws –
*State Statutes:*
Education Code, section 67100
Information Practices Act of 1977 (Civil Code section 1798)
Public Records Act (Gov. Code section 6250
Penal Codes, Section 502
*Federal Statutes:*
Federal Family Educational Rights and Privacy Act of 1974
Federal Privacy Act of 1974
Electronic Communications Privacy Act of 1986

It is probable that during employment with the McFarland Unified School District, employees will have access to either student or employee and business information that is confidential. It is the responsibility of employees to safeguard confidential information from unauthorized persons. Employees shall not seek to use personal or confidential information for their own use or personal gain. Employees must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, magnetic tape, email, etc.), paper, photograph, and microfiche information. Included under this precaution is the disposal of any privacy related materials.

## PERSONAL USE

Employees shall use district EIR primarily for purposes related to their employment. District laptop computers and portable electronic devices shall be used solely by authorized employees and not by family members or other unauthorized persons. When approved by the employee's supervisor in advance, an employee may make minimal personal use of district EIR as long as that use does not violate this

policy, does not result in any additional fee or charge to the District, and does not interfere with the normal business practices of the District or the performance of the employee's duties. Should an employee use district EIR to access personal software, websites, Apps, social media, or other personal accounts, the employee shall be responsible for any disclosure of district electronic records, including student records, resulting from that use. As described in this policy, employees have no privacy whatsoever in their personal use of district EIR, including but not limited to software, data and image files, internet use, text messages, and emails. As noted in this policy, all emails sent and received via the district email system are captured and retained by the District.

## Employee Obligations and Responsibilities

Employees are expected to use district EIR safely, responsibly, and primarily for work-related purposes. While automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources, the primary responsibility for maintaining the security of this information and its resources lies with the employee. Improper use of any of these resources can cause problems related to the needs of some or all employees and students in the District. Any incidental personal use of district EIR shall not interfere with district business and operations, the work and productivity of any district employee, or the safety and security of district EIR. The employee in whose name district technology is issued is responsible for its proper use at all times. Employees are prohibited from using district technology for improper purposes, including, but not limited to, use of district technology to:

1. Employees are prohibited from using district EIR for knowingly transmitting, receiving, or storing any oral or written communication that is obscene, threatening, or disruptive, or that reasonably could be construed as discrimination, harassment, bullying, or disparagement of others based on actual or perceived characteristics of race, ethnicity, religion, color, national origin, nationality, ancestry, ethnic group identification, physical disability, mental disability, medical condition, marital status, sex, age, sexual orientation, gender, gender identity, gender expression, genetic information (or association with a person or group with one or more of these actual or perceived characteristics). This prohibition applies to written and oral communication of any kind, including music and images.
2. Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from a supervisor
3. Infringe on copyright, license, trademark, patent, or other intellectual property rights
4. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission, changing settings on shared computers)
5. Install unauthorized software
6. Employees are prohibited from using district EIR for knowingly accessing, transmitting, receiving, or storing any image file that depicts actual or simulated torture, bondage, or physical abuse of any human being or other creature, or that is sexually explicit or pornographic. This prohibition does not apply to technology department employees engaged in authorized tracking, investigative activities regarding technology usage history of another employee.

A. "Sexually explicit" means a visual depiction of actual or simulated human sex acts, or the unclothed human genitalia, pubic area, anus, buttocks, or female breast that lacks serious artistic, literary, scientific, or political value.

B. This prohibition applies to visual depictions of any kind, including screensavers, drawings, cartoons, and animations.

7. Employees shall not knowingly store, transmit, or download copyrighted material on EIR without permission of the copyright holder. Employees shall only download copyrighted material in accordance with applicable copyright laws.

8. Employees are prohibited from knowingly using EIR to intentionally access information intended to be private or restricted; change data created or owned by another user or any other agency, company, or network; make unauthorized changes to the appearance or operational characteristics of the District's system; load, upload, download, or create a computer virus; alter the file of any other user or entity; remove a password; or alter system settings, preloaded software settings, firmware, and hardware without prior approval of the designated technology administrator at the employee's worksite.
9. Employees are prohibited from remotely accessing the district electronic network without prior express approval of the Superintendent or designee.
10. Employees are prohibited from uploading to a non-district server any file contained on a district computer or server; whether the file is work related or personal, without prior approval of the designated technology administrator at the employee's worksite. This prohibition is not intended to prevent uploads or file copying for appropriate work related purposes.
11. Any text transmission concerning a district matter should be done using an authorized district messaging system and/or device, or in a manner that protects the confidentiality and/or future recoverability of the message.
12. Employees also are prohibited from using EIR for the following:
• Personal financial gain
• Commercial advertising
• Political activity as defined in California Education Code Sections 7050-7058
• Religious advocacy
• Promoting charitable organizations without prior authorization
• Communicating in someone else's name
• Attempting to breach network security
• Creating, sending, or receiving materials that are inconsistent with the mission and values of the District
• Mass distribution of email to a school site without prior approval of the site administrator
• Mass distribution of email to the District without approval of the Superintendent or designee
• Any activity prohibited by law, board policy, administrative regulation, or the rules of conduct described in the Education Code
13. Employees are prohibited from using personal computers, devices, or internet connections for any unacceptable use identified in this policy while physically located on or in a district facility.

## No Possessory Interest

I understand that I have no specific ownership or possessory right in the District device I use or in the information stored or created therein. The Device is the property of the District. This Device and the information contained therein may be assigned or used by other employees, on as-needed basis, in furtherance of the District's operational and administrative objectives. I further understand that the District has the right and does periodically upload information from my device to District maintained servers and databases and that my internet use may be monitored and restricted by District filtering devices.

## District Access to Device

I recognize that the District will periodically access my EIR to perform the following functions:
a) Repairs or maintenance of the device.
b) Upgrading of device.

c) Retrieval of information in response to Public Records Act.
d) Retrieval of record in compliance with the Pupil Record Act, Education Code section 49062, et seq., FERPA and AB 1584.
e) Fulfill the District's statutory duties and Board policies to maintain public records.
f) Conduct administrative searches of the device.
g) Monitor employee compliance with state and federal law and District policy.

### Personally Owned Devices

If an employee uses a personally owned device to access district EIR or conduct district business, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

## Records

Any electronically stored information generated or received by an employee which constitutes a district or student record shall be classified, retained, and destroyed in accordance with BP/AR 3580 - District Records, BP/AR 5125 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.

## Software Copyright Law

Violations of copyright law have the potential of exposing the McFarland Unified School District substantial risk of liability for damages. Employees are prohibited from installing any software without having proof of licensing. Employees may not install software licensed for one workstation on multiple machines. Employees should be aware that if, for example, a department purchases a new workstation, the program must also purchase new software licenses for the software that will be installed on it. If the computer being replaced will be retired from use, the software may be removed from it and transferred to a new workstation.

## Use of the Internet

The Internet provides an extremely valuable resource for learning and communicating with people throughout the world. It can be a marvelous tool to enhance student and staff education and productivity. Unfortunately, the Internet also contains a large amount of information that is inappropriate for use in an educational institution. Employees are not to let personal use of the Internet encroach on or displace time spent performing their work duties. Inasmuch as every transaction completed on the Internet represents to the world our District and everything it stands for, it is imperative that employees not use the Internet in such a way as to bring civil or criminal liability or public reproach upon the McFarland Unified School District.

## Your Computer Account

In order to utilize the McFarland Unified School District’s computer and network resources, employees will be assigned “user IDs” and passwords. Based on an employee’s position and his or her supervisor’s authorization, the employee may be provided with access levels, which allow him, or her to view, create, alter, delete, print, and transmit information.

Employees are responsible for maintaining the security of their personal account and may not release it for use by any other individual. Employees must accord a user account the same significance as a hand-written signature. Failure to do so by releasing this information to another individual may be considered false representation and result in disciplinary action. This means that it is extremely important that employees use a password that cannot be guessed by others through knowledge about the employee. Employees should contact their site administration if they suspect someone else may have accessed their account. It is a simple matter to change a password in a few seconds, but may take days to reconstruct damaged records or computer systems if someone breaks in with employee account rights!

Only assigned employees may have direct publishing (write privilege) access to McFarland Unified School District and individual schools web, mail, and servers in general. Those who assume responsibility for posting information must never delegate these responsibilities. Passwords may not be stored where students may have access to them. Passwords should be periodically changed.

## Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, and other damaging programs that attack computer and network resources. The McFarland Unified School District attempts to maintain anti-virus software in order to minimize impact of these viruses, but it is your responsibility to take precautions to protect your computer and all others throughout the McFarland Unified School District. Employees should be very aware of opening email attachments. When in doubt, they should NOT be opened.

Likewise, employees should not download any software from the Internet unless directed to and authorized by the McFarland Unified School District Administration. It is not unknown for even a very respectable company to unknowingly release products which include hidden or unknown viruses. Employees should not share any downloaded software with others until they have verified that it does not harbor viruses or malicious software, and the software has been approved by the administrator of the designated site/department.

## Electronic Mail

The McFarland Unified School District encourages the use of email to enhance communication and business activities. The nature of electronic mail at this date makes it susceptible to misuse. Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both within the McFarland Unified School District as well as externally throughout the world. In addition, while email accounts may be password protected, it is up to the individual user to ensure that a password is set and that the password is one that cannot be easily guessed or “hacked”.

Because of backup procedures in force with the McFarland Unified School District, the fact that you have “deleted” an email message does not necessarily mean that it cannot be retrieved. Users of the McFarland Unified School District’s email services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All email sent or received by individuals through McFarland Unified School District employee accounts is the property of the McFarland Unified School District and may be requested by your supervisor and examined.

There is no guarantee that email received was in fact sent by the purported sender, since it is a simple matter, although a violation of this policy, to disguise the sender’s identity. Furthermore, email that is forwarded may be modified by the forwarder. As with any document, if you receive a message which appears unusual or which you feel may be questionable, check with the purported sender to verify authorship and authenticity.

While the McFarland Unified School District does not have the time nor inclination to monitor or read individual email messages, in the event that questionable or inappropriate use is suspected or known, such email may be examined and may be cause for disciplinary action ranging from revoking your email

account up to termination. Users should also be aware that in the general course of business, System Administrators and email operators may require observation of messages in order to verify system operation.

The confidentiality of electronic mail cannot be assured. Users should exercise extreme caution in using email to communicate confidential or sensitive material.

SOFTWARE AND ELECTRONIC DEVICES

Software, computers, and electronic devices must meet specific standards to protect the District's electronic network and other EIR.

Computers, cellphones, tablets, and similar devices are capable of downloading, storing, and using various software, including Apps, from both district-approved and non-approved providers. Some Apps are known to collect data from devices onto which they are loaded and from other devices to which the device is connected. That collection, and any dissemination of collected data, is a threat to the confidentiality of electronic records stored on district EIR and a breach of information security. For this reason, employees shall not download non-approved Apps onto district computers or devices. If an employee downloads a non-approved App onto a district computer or device, the employee may be held personally liable for any resulting unauthorized disclosure of district electronic records, including student records, in addition to any disciplinary actions taken for the unauthorized download.

Employees are discouraged from downloading non-approved Apps onto personal computers and devices that may contain district electronic records or be connected to or used with district EIR. Employees are responsible to ensure that no district electronic records are compromised and no confidential information is inappropriately disclosed or breached because of the employee's use of personal computers or devices or any software downloaded onto them.

The Superintendent/designee is authorized to approve employee requests for installation of non-district software onto district computers and devices, subject to the following limitations:

1. Software not related to the mission of the District shall not be installed.
2. No software shall be installed without written proof of licensing, which shall be retained by the technology administrator. Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.
3. Approval shall be limited, as follows:

• The District has the right to remove the software at any time and for any reason without prior notice to the employee.
• The District has no obligation to return the software to the employee.
• If the employee is assigned to a different computer or electronic device, the District has no obligation to install the software on that equipment.

Employees who have been authorized to download and install software shall adhere to copyrights, trademarks, licenses, and any contractual agreements applicable to the software, including provisions prohibiting the duplication of material without proper authorization and/or inclusion of copyright notices in any use of the material.

FILTERS AND OTHER INTERNET PROTECTION MEASURES

To ensure that use of the District's network is consistent with the District's mission, the District uses content and/or bandwidth software to prevent access to pornographic and other websites that are inconsistent with the mission and values of the District. No employee shall bypass or evade, or attempt to bypass or evade, the District's filter system. This prohibition includes the use of personal computers, devices, or internet connections to access inappropriate content while in a district facility.

**APPROPRIATE USE OF PERSONAL COMPUTERS AND DEVICES, PUBLIC RECORDS, AND COLLECTION OF DISTRICT ELECTRONIC RECORDS**

To the extent described, this policy also applies to an employee's personal computer or electronic device that either contains district electronic records or is being used with or connected to district EIR, and also applies to the use of personal computers and devices while they are physically located on district property. Without limitation, this includes personal cellphones or other devices, the use of which is supported by a district stipend.

While use of personal computers and other personal devices for district business is permitted, it is also discouraged. Employees are advised that any and all district electronic records contained on any personal device are the property of the District and their disclosure may be required. Employees *have* no expectation of privacy in such records. District business communications and records may constitute "public records" under the California Public Records Act, and may be records which the District is required to maintain under applicable law, including Title 5 of the California Code of Regulations. The District may be required to collect, disclose, produce and/or store such records, regardless of the ownership of the computer or device on which the records are located. There is no expectation of privacy in any public record located on a personal computer or device. Upon request, employees will search personal computers, personal devices, and personal email and messaging systems for the presence of district electronic records and deliver them to the District.

For example, use of an employee's personal email account to send or receive email related to district business could result in the personal email account containing records potentially deemed to be public records subject to collection and disclosure or district retention and such email shall be forwarded to the district email system, unless the email already reflects it is sent from or is copied to the district email system. The forwarded or copied email becomes the official district record of the email, will be retained by the district email system, and such email on the employee's personal email system, and/or reflected in the personal computer or device, would only be only a duplicate copy, not subject to required collection in response to a public records request, and should thereafter be deleted from the employee's personal email account. In such instances, there should be no expectation of privacy in the email.

If the employee works on, prepares, creates, or possesses an electronic record pertaining to district business, in any form, on a personal computer or device, that record would potentially be deemed a public record or record subject to collection, disclosure, or district retention. In those instances, there should be no expectation of privacy in the district electronic record located on an employee's personal computer or device in any form or formal. Upon request, the employee shall transmit the record in electronic format to the District, either through use of the district email system or other means, and then delete the record from the employee's personal computer or device.

When an employee is requested to search for public records on a personal computer or device, a personal server, or in personal email or other accounts, the employee shall conduct a search for the records in a timely manner and may report on the search results in one or more of the following ways:

1) Delivering the located public records to the District, or

2) Providing an affidavit stating that no public records were found, or

3) Providing an affidavit with sufficient information about a record to show it should not be deemed a public record.

Only the District's designated chief technology administrator is allowed to authorize installation or maintenance of either hardware or software on district or personal computers and electronic devices, with the following exceptions:

• Employees required by the District to have personal electronic devices may install such connection software as required to permit uploading, downloading, and syncing their required devices with a district computer;

• Employees required by the District to have personal electronic devices will be provided authorized software, including authorized Apps for the devices; downloading non-authorized Apps onto such devices is discouraged;

• Employees authorized to connect personal electronic devices to district EIR may be required to install appropriate security protection software on the device and the chief technology administrator may, in his/her discretion, elect to provide the required security protection software.

Certain activities on personal computers or devices while those devices are physically located on district property or sites may be permissible as long as those activities do not violate this policy, do not result in any additional fee or charge to the District, and do not interfere with the normal business practices of the District or performance of the employee's duties. For example only, while physically located on or in a district facility, employees may use a personal device to check personal email or take a call.

**NOTICE REGARDING USE OF GOOGLE AND OTHER THIRD PARTY "CLOUD" PRODUCTS AND SERVICES**

1. The District has elected to use a variety of outside vendors who provide websites, web-based software, and other services which may include mobile Apps, all of which are referred to as "cloud" services. The District is using various cloud products and services, including Google products and services, for both internal purposes and instructional use with students. As providers of those products or services, these vendors are acting as school officials under contract for the required services. Student records may properly be shared with school officials, including district employees and others who have a legitimate educational or other legally authorized purpose and who may need the records to perform the tasks for which they are employed or contracted.

Outside vendors who may have access to particular records have a formal written contract with the District to provide defined services or functions outsourced by the District, and may include consultants, insurance carriers, claims adjusters, accountants, attorneys, investigators, or others, including third party cloud vendors and service providers of online educational software and/or services that are part of the District's educational program, or who manage certain data stored in a secure cloud computing or web-based system for the District (e.g., Google is a third party vendor/school official).Written contracts for third party cloud providers include significant privacy requirements intended to protect student information from unauthorized disclosures and uses. While the District endeavors to protect student information, the use of internet connections and the presence of links in online products and services, the ease in accessing other websites and services without such protections, the potential presence of unapproved Apps on computers and devices, and the ability of students and others with lawful access to inappropriately use or share student information outside the District's control will always be present. The District intends that no student information will be inappropriately shared or used. For confidentiality purposes, student information includes both "personally identifiable information" and "covered information." Both personally identifiable and covered information are routinely disclosed to school officials in the course of initiating and using cloud services.

• "Personally identifiable information" includes but is not limited to a student's name, the name of the student's parents or other family members, the student's address, a personal identifier(such as the student's social security number), student number or biometric record, indirect identifiers(such as the student's date of birth, place of birth, and mother's maiden name), other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person-in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the agency reasonably believes knows the identity of the student to whom the education record relates.

• "Covered information" includes personally identifiable information or materials in any media or format that is created or provided by a student, or the student's parent or legal guardian, or is created or provided by an employee or agent of the District, or which is descriptive of a student or otherwise identifies a student, including educational records or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

2. Employees should make themselves aware of the presence or absence of student information in their use of Google products and services. Any communication containing student information made with persons inside or outside the District, including via email or any Google application for sharing information, should be made only with persons legally entitled to receive the student information without violating rules against unauthorized disclosure. Student information shared by an employee with anyone outside the District without express permission from the designated technology administrator at the employee's worksite is shared at the employee's own risk.
3. Employees will only log in to district Google products and services using their assigned district Google log-in information, which will be different from their regular district log-in information; employees will not log in to district Google products and/or services using any personal or non-assigned Google log-in information.
4. Employees will not log in to district Google products and services using any personal computer or personal device that contains non-district Google products or services without express permission from the designated technology administrator at the employee's worksite.
5. When using district Google products and services, employees may be exposed to links to other Google applications that are not part of the G Suite core applications or sites. Those linked applications and sites are not required to be secure or confidential and may collect and share sensitive information, including student educational records, student covered information, or employee sensitive information. Employees will not use links or access non-G Suite applications or sites and will immediately exit any linked applications or sites if accessed.
6. Employees understand that their use of district EIR is subject to this policy and that its terms take precedence over anything to the contrary contained or represented in any Google documents or policies.
7. Employees understand that email and documents created within district Google products and services are not maintained in or on district EIR, that they are stored within the architecture of the Google products and services and that the District has no control over the safety, security, or maintenance of the email and documents. Email and documents pertaining to the business of the District, including student instructional material, may be public records and may be records that are required to be retained and employees shall not delete or discard public or other records that require retention by the District.
8. Employees who are designated as or otherwise become administrators of a Google network within the District shall make all privacy and other settings the most restrictive and protective of student information unless expressly authorized not to do so by an administrator at district cabinet level.
9. Employees working with a district Google application shall not attempt to bypass or avoid the privacy settings of the application.

**DISCLAIMER**

The District makes no guarantees about the quality of the EIR provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from employee use of district EIR. Any charges an employee accrues due to personal use of district EIR are to be borne by the employee. The District also denies any responsibility for the accuracy or quality of the information obtained through employee access.

**VIOLATION OF THIS POLICY**

Violation of this policy shall be promptly reported to management personnel. Management personnel shall then promptly report any violation of this policy to the Superintendent or designee. Employees who violate this policy are subject to discipline, up to and including termination, pursuant to the provisions of applicable laws governing employee discipline and applicable district policies, procedures, and collective bargaining agreements. An employee's use of district EIR may also be restricted, suspended, or revoked.

# EMPLOYEE USE OF TECHNOLOGY
# ACCEPTABLE USE AGREEMENT FORM

## SUMMARY OF POLICY

Significant components of the Employee Use of Technology Acceptable Use Agreement include but are not limited to the following, which are intended only to highlight (and summarize but not define) some of the rules contained in the Policy:

- Employees have absolutely no expectation of privacy in their use of any District electronic information resources ("EIR"), including email or in District electronic records located on personal computers and other devices
- Employees are to use District EIR in furtherance of the District's mission and not in any way not in furtherance of the mission
- Employees' personal devices, including computers, cellphones, "smartphones", and tablets (iPad, Nook, Kindle, etc.), are covered by many aspects of the Policy
- Installing/downloading commercial software applications (Apps) is prohibited for District devices and is discouraged for any personal devices that will be connected in any way to District EIR. Connection of personal devices to District EIR, including flash or thumb drives and collected data relating to the connection, will be monitored.
- Employees' personal email sent or received using District EIR is being captured and stored
- Employees must use password and other protections for personal computers and devices used for District-related purposes
- Employees may not bypass or evade, or attempt to bypass or evade, District filtering systems
- Violations of the Policy may lead to discipline, up to and including dismissal from employment

## EMPLOYEE COMPLIANCE AGREEMENT

I have read, understand, and agree to abide by the provisions of the entire Employee Acceptable Use Policy for Computers, Electronic Devices, Network, and Other Electronic Information Resources which has been made available to me either or both in hard copy and/or electronic format, and which I understand remains available for review on the District's website. I understand use of District EIR is a privilege, not a right, and that I have no expectation of privacy in my use of District EIR, and that my misuse may result in restriction or cancellation of my usage privileges and lead to disciplinary and/or legal action, as set forth in the Policy. I will transfer from my personal devices all District-related records.

Name: _____ Site: _____

Signature: _____ Date: _____

Position: _____ Classified:_____ Certificated:_____