Access to Electronic Media

(Acceptable Use Policy)

The Board supports reasonable access to various information formats for students, employees and the community and believes it is incumbent upon users to utilize this privilege in an appropriate and responsible manner as required by this policy and related procedures, which apply to all parties who use District technology. This access is offered through the JCPS Networks.

Communication, data, and files transferred through the JCPS are not private. They may be reviewed by specific District personnel, or by someone appointed by them (i.e., independent contractors, law enforcement, etc.), to ensure that all Board policies, administrative procedures, and state and federal laws are followed. Violation of this policy may result in disciplinary action in accordance with the Student Support and Behavior Intervention Handbook, agreements with employee organizations, and Board policies relating to personnel matters.

STUDENT SAFETY PROCEDURES AND GUIDELINES

The Superintendent/designee shall develop and implement appropriate administrative procedures to provide guidance for access to electronic media. Procedures shall address teacher supervision of student computer use, ethical use of electronic media (including, but not limited to, the Internet, e-mail, and other District technological resources), and issues of privacy versus administrative review of electronic files and communications.

Students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in digital messaging, and cyberbullying awareness and response.

Internet safety measures, which shall apply to all District-owned devices with Internet access or personal devices that are permitted to access the District's networks, shall be implemented that effectively address the following:

- Controlling access by minors to inappropriate matter on the Internet;
- Safety and security of minors when they are using electronic mail, digital messaging, and other forms of direct electronic communications;
- Preventing unauthorized access, including "hacking" and other unlawful activities by minors online;
- Unauthorized disclosure, use and dissemination of personal information regarding minors; and
- Restricting minors' access to materials harmful to them.

STUDENT USE

This Student Acceptable Use Policy is included in the Student Support and Behavior Intervention Handbook (SSBIH) which is provided to all students at the beginning of each school year. Parents/guardians and students are expected to sign an acknowledgement of receipt of the SSBIH and affirm that they have read and discussed its contents.. Failure to sign the acknowledgement does not relieve students of the requirement to adhere to the provisions of the SSBIH.

A technology protection measure may be disabled by the Board's designee during use by an adult to enable access for bona fide research or other lawful purpose.

Access to Electronic Media
(Acceptable Use Policy)

STUDENT USE (CONTINUED)

Students are responsible for appropriate behavior when using the JCPS Networks and other District resources, just as they are in classrooms and school hallways. Therefore, general school rules for expectations and District behavior guidelines apply. Access to network services is provided, and students are expected to act responsibly. Based on the acceptable use guidelines outlined in this policy, the system administrators will deem what is inappropriate use, and their decisions are final.

The administration and staff may revoke or suspend user access when these terms are violated.

A Student shall:

- Follow school and District behavior expectations to be a respectful and responsible digital citizen.
- Use all online, cloud, and network resources and accounts as instructed and for educational purposes.
- Store and share only appropriate material.
- Use school and/or personal technology only at approved times for appropriate purposes.

A Student shall NOT:

- Access, send or willfully receive any content that is inappropriate, offensive, harassing, or profane in nature or that which promotes violence or illegal activity, except in support of a legitimate educational purpose, which is permitted with teacher approval and oversight.
- Willfully waste resources or use them for non-academic purposes (e.g., file storage, printing, bandwidth, etc.)
- Use or share the student's or another person's username or password with others.
- Compromise the JCPS Networks and their settings in any way (e.g., hacking, spamming, bypassing security, etc.)
- Use the JCPS Networks for personal gain, entertainment, political promotion, or activities unrelated to school, except for incidental personal use, which is permitted.
- Violate copyright laws or commit plagiarism, including the copying of software, music, or other copyright protected files.
- Intentionally damage or steal District or personal technology-related property.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Create, download, view, store, copy or transmit content generated with an Artificial Intelligence (AI) system in an inappropriate or unethical manner, including, but not limited to:
    - Fraudulent activity, including but not limited to impersonating individuals or organizations to steal money, information, or other assets.
    - Harassment or discrimination.
    - Impersonation: Creating AI-generated audio or video to mimic real people.

Access to Electronic Media
(Acceptable Use Policy)

A Student shall NOT: (continued)

- Appropriated likeness: Using or altering a person's likeness without consent.
- Creating a false online persona to deceive or manipulate others or spread false information (i.e. sockpuppeting).
- Generating explicit content.
- Plagiarism.
- Cheating on assessments or assignments by representing AI-generated content as the student's own.
- Using AI to bypass plagiarism-detection software.
- Falsification: Using AI to fabricate evidence such as reports or documents.
- Intellectual property (IP) infringement: Using someone's intellectual property without permission.
- Counterfeiting: Producing items that imitate original works and attempt to pass as real.
- Scaling and amplification: Automating and amplifying content distribution.

STUDENT INDEPENDENT RESOURCE OPT-OUT

Computers and mobile device use is a vital part of the District's instructional plan, particularly in presenting personalized learning opportunities for all students.

Students may be assigned a device to gain knowledge, develop skills, and extend the student's current capabilities. Student devices may be used daily to support and guide learning within the District's instructional plan, which encompasses both school use and use beyond the school day or outside of the school setting, including, but not limited to, use in the provision of Extended School Services (ESS); and use on Non-Traditional Instructional (NTI) days. These resources are for academic purposes only. While using these resources, a student must abide by the JCPS Student Support and Behavior Intervention Handbook, the JCPS Student Acceptable Use Policy, and applicable state and federal laws.

For a student to opt out of use of District technology resources outside of the District's instructional plan, including non-NTI home-based use, a parent/guardian must provide written notice to the school Principal. The student will still use District-provided technology resources in the classroom, for ESS services, and on NTI days, as part of the District's instructional plan.

EMPLOYEE USE

Overview

The District recognizes the value of information systems, applications, and data as well as computers, storage, network, and other electronic devices to improve and enhance student learning. To this end, the District encourages the responsible use of these computing equipment resources in support of the educational mission and goals of the District.

Access to Electronic Media

(Acceptable Use Policy)

The JCPS Networks help employees carry out the District's educational mission, conduct research, and communicate with others about District work. Along with this access comes the availability of materials that may not be considered appropriate for use in the workplace. Because it is impossible to control all materials available through the Internet, each employee is ultimately responsible for observing the JCPS standards outlined below, as well as other applicable school and District rules for behavior and communications.

The District has drafted this policy governing the voluntary use of computing resources, to provide guidance to District employees regardless of whether the District provides the equipment, or the individual/group obtains the same through donations from any organization.

Purpose

The purpose of the Employee Acceptable Use Policy to establish acceptable and unacceptable use of any computing device or electronic resource listed as part of the Acceptable Use Agreement. All users of computer equipment listed, including but not limited to, servers, both wired and wireless networks, storage media, as well as software, operating systems, accounts, and any type of system installed on this equipment on District premises, are covered by the Agreement. It is the responsibility of every employee to know and understand the Agreement and to conduct their activities accordingly.

Scope

All District employees, including all personnel affiliated with the school that will be using the computing equipment listed, shall adhere to the Agreement. Employees are required to sign the Employee Acceptable Use Agreement (Administrative Procedure 05.51 AP.21) at the beginning of each contract year acknowledging they have read and agree to comply with the Employee Acceptable Use Agreement. New employees are required to sign the Employee Acceptable Use Agreement upon being hired.

This Employee Acceptable Use Policy applies to the use of the District-provided IT resources, regardless of the geographic location, as follows:

- Data and system use shall comply with the District standards found in the Board-approved policies and administrative procedures.
- Unauthorized access to data and/or systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information/data, including Personally Identifiable Information (PII).
- While using the District network, users should have no expectation of privacy. The District has the right to monitor all traffic on the District network.

Access is a privilege, not a right.

Access to this shared resource is given to employees who agree to utilize the JCPS Networks to support the educational business of the District and to act in a considerate and responsible manner.

Access to Electronic Media

(Acceptable Use Policy)

ACCEPTABLE USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA

An Employee shall:

- In accordance with District administrative procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information or data, including PII, maintained or in possession of the user.
- Ensure that software, including downloaded software and cloud services, are properly licensed, free of malicious code, and authorized for installation and use before installing or using it on organization-owned systems.
- Log off or lock systems when leaving them unattended.
- Complete security awareness training before accessing any system and on an annual basis thereafter. Permit only authorized users to use organization-provided systems.
- Secure sensitive information or data (on paper and in electronic formats) when left unattended.
- Keep sensitive information or data out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with organization records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information or data necessary to perform job functions and for which the user has appropriate access authorization from the District.
- Use PII only for the purposes for which it was collected, including conditions set forth by stated privacy notices and published notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as necessary.

PROHIBITED USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA

An Employee shall NOT:

- Access and/or share information or data outside the purview of their job function, except that incidental personal use is permitted.
- Direct or encourage others to violate District policies, administrative procedures, standards, or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of the principle of least privilege).
- Use another user's account, identity, or password.
- Exceed authorized access to sensitive information or data.

Access to Electronic Media
(Acceptable Use Policy)

PROHIBITED USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA (CONTINUED)

- Cause congestion, delay, or disruption of service to any District-owned IT resource. For example, sending greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network, as does some uses of "push" technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually oriented materials.
- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities, or activities otherwise prohibited.
- Create, download, view, store, copy or transmit content generated with an Artificial Intelligence (AI) system in an inappropriate or unethical manner, including, but not limited to:
    - Fraudulent activity, including but not limited to impersonating individuals or organizations to steal money, information, or other assets.
    - Harassment or discrimination.
    - Impersonation: Creating AI-generated audio or video to mimic real people.
    - Appropriated likeness: Using or altering a person's likeness without consent.
    - Creating a false online persona to deceive or manipulate others or spread false information (i.e. sockpuppeting).
    - Generating explicit content.
    - Falsification: Using AI to fabricate evidence such as reports or documents.
    - Intellectual Property (IP) infringement: Using someone's intellectual property without permission.
    - Counterfeiting: Producing items that imitate original works and attempt to pass as real.
    - Scaling and amplification: Automating and amplifying content distribution.
- Store sensitive information or data in public folders or other insecure physical or electronic storage locations.
- Share sensitive information or data, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Disclose student educational records, including any student information or data, except as permitted by the Family Educational Rights and Privacy Act (FERPA), state and federal law, and the District Board policy.

Access to Electronic Media
(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

- Transport, transfer, email, remotely access, or download sensitive information or data, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information or data.
- Store sensitive information/data on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information /data for personal use for self or others.
- Use organization-provided IT resources for commercial purposes, in support of "for-profit" activities, or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).
- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- Establish unauthorized personal, commercial, or non-profit organizational web pages on organization-provided systems.
- Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.
- Use organization-owned IT resource for activities that are inappropriate or offensive. Such activities include, but are not limited to:
    - Harassment, bullying, intimidation, or use of any term or image designed to insult others, based on race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex (including sexual orientation and gender identity), gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions of an employee.
    - Hate speech;
    - Nudity, obscenity, and/or vulgarity;
    - Discussion of conduct illegal for a minor; and
    - Promotion or depictions of illegal conduct, including drug or inappropriate alcohol use.

Access to Electronic Media
(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

- Add personal IT resources to existing organization-owned systems without the appropriate management authorization, including the installation of personal networks and reconfiguration of systems.
- Intentionally acquire, use, reproduce, transmit, or distribute any controlled information or data including computer software and data that includes information or data subject to FERPA, HIPPA, the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.
- Send anonymous messages.
- Remove organization-approved IT resources from organization property without prior management authorization.
- Modify software without management approval.
- Implement the use of purchased or free software, including enrolling, rostering, or sharing any student data as part of a course curriculum without successful completion of the District digital resource review process.
- Share any exploits or compromises discovered in the network or systems. If one is discovered, it should be reported to the IT department immediately.
- Post information or data on external blogs or social media including, but not limited to, networking sites, newsgroups, bulletin boards or other public forums in a manner that violates Board policy.

USE OF TECHNOLOGY IN THE CLASSROOM

Employees are encouraged to use electronic mail and other District technology resources to promote student learning and for communication with parents and education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities.

Technology-based materials, activities and communication tools shall be appropriate for and within the range of the knowledge, understanding, age and maturity of students with whom they are used.

SOCIAL NETWORKING SITES

An employee may set up social networking accounts using District resources and following District procedures to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

Networking, communication, and other options offering instructional benefits may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.

In order for an employee to utilize a social networking site for instructional, administrative, or other work-related communication purposes, he/she/they shall comply with the following:

1. Request prior permission from the Superintendent/designee.

Access to Electronic Media
(Acceptable Use Policy)

SOCIAL NETWORKING SITES (CONTINUED)

2. If permission is granted, set up the site in accordance with following District guidelines developed by the Superintendent/designee. Guidelines may specify whether access to the site must be given to school/District technology staff.
3. Notify the parent/guardian of each participating student of the site and obtain written permission for students to become "friends" prior to a student being granted access. This permission shall be kept on file at the school as determined by the Principal.
4. Once the site has been created, the sponsoring employee shall be responsible for the following:
   a. Monitoring and managing the site to promote safe and acceptable use; and
   b. Observing confidentiality restrictions concerning release of student information under state and federal law.

An employee is discouraged from creating or using a personal social networking site to which they invite students to be friends. An employee who takes such action does so at their own risk.

An employee shall be subject to disciplinary action if the employee's conduct relating to use of technology or online resources violates this policy or other applicable policy, administrative procedure, or statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of that Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to the Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

COMMUNITY USE

On recommendation of the Superintendent/designee, the Board shall determine when and which computer equipment, software, and information access systems will be available to the community.

The District may provide Wi-Fi internet access for guests to schools and other District facilities that may be used without prior approval. With the approval of the Principal/designee, a community member may be granted access to District electronic information sources and programs available through the District's technology system, provided he/she/they attend any required training and abide by the rules of usage established by the Superintendent/designee.

An employee or student shall be subject to disciplinary action, up to and including termination (employee) or placement in an alternative program or setting in lieu of expulsion (student) for violating this policy and acceptable use administrative procedures established by the District.

Access to Electronic Media
(Acceptable Use Policy)

RESPONSIBILITY FOR DAMAGES

An individual shall reimburse the Board for repair or replacement of District property lost, stolen, damaged, or vandalized while under their care. A student or staff member who defaces a District web site or makes unauthorized changes to a web site shall be subject to disciplinary action, up to and including placement in an alternative program or setting in lieu of expulsion or termination, as appropriate.

RESPONDING TO CONCERNS

A school or District administrator shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

AUDIT OF USE

A user with network access shall not utilize District resources to establish electronic mail accounts through a third-party provider or any other nonstandard electronic mail system.

The Superintendent/designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters internet access for both minors and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;
2. Maintaining and securing a usage log; and
3. Monitoring online activities of minors.

RETENTION OF RECORDS FOR E-RATE PARTICIPANTS

Following initial adoption, this policy and documentation of implementation shall be retained for at least ten (10) years after the last day of service in a particular funding year.

ADDITIONAL RULES FOR SECURITY AND PRIVILEGED USERS

Certain security and system administration personnel are granted elevated privileges by the Chief Information Officer/designee. Elevated privileges establish specific job-related roles and permissions for an employee and may provide significant access to processes and data in District systems. As such, Security, Network, Systems, and Database Administrators have added responsibilities to ensure the secure operation of any the District systems.

Personnel with elevated privileges are to:

- Advise the asset owner on matters concerning cybersecurity.

Access to Electronic Media
(Acceptable Use Policy)

ADDITIONAL RULES FOR SECURITY AND PRIVILEGED USERS (CONTINUED)

- Assist the asset owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to any system that affect contingency and disaster recovery plans are conveyed to the asset custodian responsible for maintaining continuity of operations plans for that system.
- Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information/data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to any system.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document any known or suspected security incidents or violations and report them to the Executive Administrator for Information Security and Cyber GRC (Governance, Risk, and Compliance) .
- Ensure the protection and security of these devices, which includes reasonable protection from any environmental elements. Promptly report any theft of these devices to the immediate supervisor or manager.

BRING YOUR OWN DEVICE (BYOD)

The purpose of the Bring Your Own Device (BYOD) policy is to specify what security measures must be in place and to define acceptable use and controls when personal devices are used to access District systems and data.

The following provisions apply to BYOD:

- Texting or emailing while driving is strictly prohibited.
- Access to the District emails and documents is only permitted as an exception to the BYOD policy if the following controls are in place:
    - The personal device is protected by a passcode.
    - The personal device is not jailbroken, (i.e., modified to remove restrictions imposed by the manufacturer or operator), (e.g., to allow the installation of unauthorized software).
- District information/data shall not be shared with or sent to an unauthorized third party.
- District confidential information/data shall be deleted from personal devices upon separation with the District.
- The District reserves the right to disconnect a personal device or disable service without notification.

Access to Electronic Media
(Acceptable Use Policy)

BRING YOUR OWN DEVICE (BYOD) (CONTINUED)

- A lost or stolen device shall be reported to the District IT Division within twenty-four (24) hours. A personal device user is responsible for notifying his/her/their mobile carrier immediately upon loss of a device.
- A personal device user is expected to use his/her/their device in an ethical manner at all times and adhere to the District's Acceptable Use Agreement as outlined in this policy.
- A personal device user is personally liable for all costs associated with the user's device.
- A personal device user assumes full liability for risks including, but not limited to, the partial or complete loss of District or personal data due to an operating system crash, errors, bugs, viruses, malware, other software or hardware failure, or a programming error that renders the device unusable.
- The District shall not reimburse an employee for the cost of a device or plan.

The District shall not be responsible for supporting a personal device including connectivity to the District systems.

The District reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with the BYOD agreement.

ACRONYMS & KEY TERMINOLOGY

The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that the District uses to define common cybersecurity terms. Key terminology includes:

- Adequate Security:
  - A term describing protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to or modification of information.
- Artificial Intelligence:
  - A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.
- Artificial Intelligence System:
  - Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.
- Asset:
  - A term describing any data, device, application, service, or other components of the environment that supports information-related activities. An asset is a resource with economic value that the District owns or controls.

Access to Electronic Media
(Acceptable Use Policy)

ACRONYMS & KEY TERMINOLOGY (CONTINUED)

- FERPA:
  - Family Educational Rights and Privacy Act (FERPA) – the federal law in the United Stated that governs the privacy of student educational records.
- IT:
  - Information Technology
- Jailbroken:
  - Modification (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, (e.g., to allow the installation of unauthorized software).
- PII:
  - Personally Identifiable Information: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
- Spam:
  - Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 5:120
16 KAR 1:020 (Code of Ethics)
47 U.S.C. 254/Children's Internet Protection Act; 45 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516

RELATED POLICIES:

03.13214/03.23214; 03.1325/03.2325; 03.17/03.27
08.1353; 08.2322
09.14; 09.421; 09.422; 09.425; 09.426; 09.4261
10.5

Adopted/Amended: 5/23/2023
Order #: 2023-78

Employee Acceptable Use Agreement

EXECUTIVE SUMMARY

Overview

The District recognizes the value of information systems, applications, and data as well as computers, storage, network, and other electronic devices to improve and enhance student learning. To this end, the District encourages the responsible use of these computing equipment resources in support of the educational mission and goals of the District.

The JCPS Networks help employees carry out the District's educational mission, conduct research, and communicate with others about District work. Along with this access comes the availability of materials that may not be considered appropriate for use in the workplace. Because it is impossible to control all materials available through the Internet, each employee is ultimately responsible for observing the JCPS standards outlined below, as well as other applicable school and District rules for behavior and communications.

The District has drafted this agreement governing the voluntary use of computing resources to provide guidance to District employees regardless of whether the District provides the equipment, or the individual/group obtains the same through donations from any organization.

Purpose

The purpose of this the Employee Acceptable Use Agreement is to establish acceptable and unacceptable use of any computing device or electronic resource listed as part of this Agreement. All users of computer equipment listed, including but not limited to, servers, both wired and wireless networks, storage media, as well as software, operating systems, accounts, and any type of system installed on this equipment on-premises at the District, are covered by this Agreement. It is the responsibility of every employee to know and understand this agreement and to conduct their activities accordingly.

Scope

All District employees, including all personnel affiliated with the school that will be using the computing equipment listed, shall adhere to this Agreement. Employees are required to sign this Employee Acceptable Use Agreement at the beginning of each contract year acknowledging they have read and agree to comply with the Employee Acceptable Use Agreement. New employees are required to sign the Employee Acceptable Use Agreement upon being hired.

This Employee Acceptable Use Agreement applies to the use of the District-provided IT resources, regardless of the geographic location, as follows:

- Data and system use shall comply with the District policies and standards found in the District Board-approved policies and administrative procedures.
- Unauthorized access to data and/or systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information/data, including Personally Identifiable Information (PII).
- While using the District network, users should have no expectation of privacy. The District has the right to monitor all traffic on the District network.

Access is a privilege, not a right.

Access to this shared resource is given to employees who agree to utilize the JCPS Networks to support the educational business of the District and to act in a considerate and responsible manner.

Employee Acceptable Use Agreement

ACCEPTABLE USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA

Employees shall:

- In accordance with District administrative procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information or data, including PII, maintained or in possession of the user.
- Ensure that software, including downloaded software and cloud services, are properly licensed, free of malicious code, and authorized for installation and use before installing or using it on the District-owned systems.
- Log off or lock systems when leaving them unattended.
- Complete security awareness training before accessing any system and on an annual basis thereafter. Permit only authorized users to use organization-provided systems.
- Secure sensitive information or data (on paper and in electronic formats) when left unattended.
- Keep sensitive information or data out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with the District records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information or data necessary to perform job functions and for which the user has the appropriate access authorization from the District.
- Use PII only for the purposes for which it was collected, including conditions set forth by stated privacy notices and published notices.
- Ensure the accuracy, relevance, and completeness of PII, as necessary.

PROHIBITED USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA

Employees shall not:

- Access and/or share information or data outside the purview of their job function, except that incidental personal use is permitted.
- Direct or encourage others to violate organizational policies, administrative procedures, standards, or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
- Use another user's account, identity, or password.
- Exceed authorized access to sensitive information or data.
- Cause congestion, delay, or disruption of service to any District-owned IT resource. For example, sending greeting cards, video, sound, or other large file

  attachments can degrade the performance of the entire network, as do some uses of "push" technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually-oriented materials.

Employee Acceptable Use Agreement

PROHIBITED USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA (CONTINUED)

- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities, or activities otherwise prohibited.
- Create, download, view, store, copy or transmit content generated with an Artificial Intelligence (AI) system in an inappropriate or unethical manner, including, but not limited to:
    - Fraudulent activity, including but not limited to impersonating individuals or organizations to steal money, information, or other assets.
    - Harassment or discrimination.
    - Impersonation: Creating AI-generated audio or video to mimic real people.
    - Appropriated likeness: Using or altering a person's likeness without consent.
    - Creating a false online persona to deceive or manipulate others or spread false information (i.e. sockpuppeting).
    - Generating explicit content.
    - Falsification: Using AI to fabricate evidence such as reports or documents.
    - Intellectual Property (IP) infringement: Using someone's intellectual property without permission.
    - Counterfeiting: Producing items that imitate original works and attempt to pass as real.
    - Scaling and amplification: Automating and amplifying content distribution.
- Store sensitive information or data in public folders or other insecure physical or electronic storage locations.
- Share sensitive information or data, except as authorized and with formal agreements that ensure third-parties will adequately protect it.
- Disclose student educational records, including any student information or data, except as permitted by the Family Educational Rights and Privacy Act (FERPA), state and federal law, and the District Board policy.
- Transport, transfer, email, remotely access, or download sensitive information or data, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information or data.
- Store sensitive information/data on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information/data for personal use for self or others.
- Use organization-provided IT resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).

PROHIBITED USE OF INFORMATION SYSTEMS, APPLICATIONS, AND DATA (CONTINUED)

- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activities.
- Establish unauthorized personal, commercial, or non-profit organizational web pages on organization-provided systems.
- Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.
- Use organization-owned IT resources for activities that are inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to:
    - Harassment, bullying, intimidation, or other abusive conduct that ridicules others on the basis of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex (including sexual orientation and gender identity), gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions of an employee.
    - Hate speech
    - Nudity, obscenity, and/or vulgarity
    - Discussion of conduct illegal for a minor; and
    - Promotion or depictions of illegal conduct, including inappropriate drug or alcohol use.
- Add personal IT resources to existing organization-owned systems without the appropriate management authorization, including the installation of personal networks and reconfiguration of systems.
- Intentionally acquire, use, reproduce, transmit, or distribute any controlled information or data including computer software and data that includes information or data subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.
- Send anonymous messages.
- Remove organization-approved IT resources from organization property without prior management authorization.
- Modify software without management approval.
- Implement the use of purchased or free software, including enrolling, rostering, or sharing any student data as part of a course curriculum without successful completion of the district software approval process.
- Share any exploits or compromises discovered in the network or systems. If one is discovered, it should be reported to the IT department immediately.
- Post information or data on external blogs or social media including, but not limited to, networking sites, newsgroups, bulletin boards, or other public forums in a manner that violates Board policy.

ADDITIONAL RULES FOR SECURITY & PRIVILEGED USERS (CONTINUED)

USE OF TECHNOLOGY IN THE CLASSROOM

Employees are encouraged to use electronic mail and other District technology resources to promote student learning and for communication with parents and education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities.

Technology-based materials, activities and communication tools shall be appropriate for and within the range of the knowledge, understanding, age and maturity of students with whom they are used.

SOCIAL NETWORKING SITES

An employee may set up social networking accounts using District resources and following District procedures to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

Networking, communication, and other options offering instructional benefits may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.

In order for an employee to utilize a social networking site for instructional, administrative, or other work-related communication purposes, he/she/they shall comply with the following:

Request prior permission from the Superintendent/designee.

1. If permission is granted, set up the site in accordance with following District guidelines developed by the Superintendent/designee. Guidelines may specify whether access to the site must be given to school/District technology staff.
2. Notify the parent/guardian of each participating student of the site and obtain written permission for students to become "friends" prior to a student being granted access. This permission shall be kept on file at the school as determined by the Principal.
3. Once the site has been created, the sponsoring employee shall be responsible for the following:
    c. Monitoring and managing the site to promote safe and acceptable use; and
    d. Observing confidentiality restrictions concerning release of student information under state and federal law.

An employee is discouraged from creating or using a personal social networking site to which they invite students to be friends. An employee who takes such action does so at their own risk.

An employee shall be subject to disciplinary action if the employee's conduct relating to use of technology or online resources violates this policy or other applicable policy, administrative procedure, or statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information.

Employee Acceptable Use Agreement

SOCIAL NETWORKING SITES (CONTINUED)

Conduct in violation of that Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to the Education Professional

Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

COMMUNITY USE

On recommendation of the Superintendent/designee, the Board shall determine when and which computer equipment, software, and information access systems will be available to the community.

The District may provide Wi-Fi internet access for guests to schools and other District facilities that may be used without prior approval. With the approval of the Principal/designee, a community member may be granted access to District electronic information sources and programs available through the District's technology system, provided he/she/they attend any required training and abide by the rules of usage established by the Superintendent/designee.

An employee or student shall be subject to disciplinary action, up to and including termination (employee) or placement in an alternative program or setting in lieu of expulsion (student) for violating this policy and acceptable use administrative procedures established by the District.

RESPONSIBILITY FOR DAMAGES

An individual shall reimburse the Board for repair or replacement of District property lost, stolen, damaged, or vandalized while under their care. A student or staff member who defaces a District web site or makes unauthorized changes to a web site shall be subject to disciplinary action, up to and including placement in an alternative program or setting in lieu of expulsion or termination, as appropriate.

RESPONDING TO CONCERNS

A school or District administrator shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

AUDIT OF USE

A user with network access shall not utilize District resources to establish electronic mail accounts through a third-party provider or any other nonstandard electronic mail system.

The Superintendent/designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

4. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters internet access for both minors and adults to certain visual depictions
5. that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;
6. Maintaining and securing a usage log; and
7. Monitoring online activities of minors.

Employee Acceptable Use Agreement

RETENTION OF RECORDS FOR E-RATE PARTICIPANTS

Following initial adoption, this policy and documentation of implementation shall be retained for at least ten (10) years after the last day of service in a particular funding year.

ADDITIONAL RULES FOR SECURITY & PRIVILEGED USERS

Certain security and system administration personnel are elevated privileges by the Chief Information Officer/designee. Elevated privileges establish specific job-related roles and permissions for an employee and may provide significant access to processes and data in District systems. As such, Security, Network, Systems, and Database Administrators have added responsibilities to ensure the secure operation of any the District systems.

Personnel with elevated privileges are to:

- Advise the asset owner on matters concerning cybersecurity.
- Assist the asset owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to any system that affect contingency and disaster recovery plans are conveyed to the asset custodian responsible for maintaining continuity of operations plans for that system.
- Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information/data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to any system.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document any known or suspected security incidents or violations and report them to the Executive Administrator for Information Security and Cyber GRC (Governance, Risk, and Compliance) .
- Employees are responsible for ensuring the protection and security of these devices, which includes reasonable protection from any environmental elements. Promptly report any theft of these devices to the immediate supervisor or manager.

Employee Acceptable Use Agreement

BRING YOUR OWN DEVICE (BYOD)

Management Intent:

The purpose of the Bring Your Own Devices (BYOD) agreement is to specify what security measures have to be in place and to define acceptable use when personal devices are used to access District systems and data.

The following provisions apply to BYOD:

- Texting or emailing while driving is strictly prohibited.

- Access to the District emails and documents is only permitted as an exception to this Agreement if the following controls are in place.
    - The Personal Device must be protected by a passcode.
    - The Personal Device cannot be jailbroken, (i.e. modified to remove restrictions imposed by the manufacturer or operator), (e.g. to allow the installation of unauthorized software).
- District information/data cannot be shared with or sent to unauthorized third parties.
- District confidential information/data shall be deleted from Personal Devices upon separation with the District.
- The District reserves the right to disconnect devices or disable services without notification.
- A lost or stolen device must be reported to the District IT within twenty-four (24) hours. Personal Device users are responsible for notifying their mobile carrier immediately upon loss of a device.
- A personal device user is expected to use their devices in an ethical manner at all times and adhere to the District's Acceptable Use Agreement as outlined in this document.
- A personal device used is personally liable for all costs associated with their devices.
- A personal device user assumes full liability for risks including, but not limited to, the partial or complete loss of the District and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The District shall not reimburse the employee for the cost of the device or plan.

The District shall not be responsible for supporting Personal Devices including connectivity to the District systems. The District reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this agreement.

ACRONYMS & KEY TERMINOLOGY

The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that the District uses to define common cybersecurity terms. Key terminology to be aware of includes:

Employee Acceptable Use Agreement

ACRONYMS & KEY TERMINOLOGY (CONTINUED)

Adequate Security:

A term describing protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to or modification of information.

Artificial Intelligence:

A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Artificial Intelligence System:

Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

Asset:

A term describing any data, device, application, service, or other components of the environment that supports information-related activities. An asset is a resource with economic value that the District owns or controls.

FERPA:

Family Educational Rights and Privacy Act (FERPA) – the federal law in the United Stated that governs the privacy of student educational records.

IT:

Information Technology

Jailbroken:

Modification (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, (e.g. to allow the installation of unauthorized software).

PII:

Personally Identifiable Information: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Spam:

Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

As an employee of the District and as a user of the District computer network, I have read and hereby agree to comply with all the District employee acceptable technology use policies, including those summarized in this Employee Acceptable Use Agreement, and Board policies 03.1321, 03.2321, and 08.2323, as applicable. I understand that if I violate any of those policies, I may lose access to the District technology resources and I may be subject to discipline, up to and including termination of employment.

Employee Name (Please print) _____

_____ _____

Employee's Signature ***Date***

Employee Acceptable Use Agreement

RELATED POLICIES:

03.1321; 03.2321; 08.2323

RELATED PROCEDURES:

08.2323 (all procedures)

Review/Revised:5/11/2021