Acceptable Use Policy for Hopkins County Schools Faculty and Staff

I. Introduction

Each employee of the Hopkins County School District is expected to be familiar with and follow the expectations and requirements of this administrative rule. The purpose of this rule is to ensure that individuals are aware of their responsibilities regarding the Internet and related technology and equipment. This rule also helps ensure the safety and privacy of current, former employees, and students.

A. Legal Requirements

HCBOE is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

1. The Family Educational Rights and Privacy Act (FERPA)
2. Children's Internet Protection Act (CIPA)
3. Individuals with Disabilities Education Act (IDEA)
4. Children's Online Privacy Protection Act (COPPA)
5. Health Insurance Portability and Accountability Act (HIPPA)

Users of HCBOE network are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies through the use of HCBOE networks may result in discipline or litigation against the offender(s) by the proper authority. HCBOE will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

B. Acceptable Use

HCBOE provides computer, network, e-mail, and Internet access to individuals as part of the learning environment. The use of these resources is a privilege and not a right. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use by every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline or litigation in accordance with board policy and state and federal law.

II. Employee Acceptable Use

This section is dedicated to provide HCBOE employees with guidance of acceptable use of the District's information technology resources, including but not limited to:

1. The internet, intranet, e-mail, district Google Drive and One Drive.
2. District assigned computing devices such as personal electronic devices, laptops, chromebooks, ipads and desktops.
3. The District's network and supporting systems and data transmitted by and stored on the HCBOE systems.

A. Prohibited Use of HCBOE Resources

The following uses of HCBOE computer resources by staff members are prohibited at all times:

1. Unauthorized or excessive personal use. Any personal use should not interfere with or impair an employee's job performance.
2. Infringing upon the intellectual property rights of others or violating copyright laws.
3. Advancing personal profit.
4. Furthering political causes in violation of board policy or the State Ethics Act.
5. Uploading or transferring out of the District's direct control any software licensed to the District or data owned by the District without explicit written authorization. Failure to observe copyright or license agreements can result in disciplinary action from HCBOE or legal action by the copyright owner.
6. Unauthorized use of resources (including but not limited to servers, networks, computers and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms.
7. Bypassing or attempting to bypass any of the District's security or content filtering safeguards.
8. Accessing or attempting to access resources for which an employee does not have explicit authorization by means of assigned user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
9. Granting another individual access to any District accounts that have been authorized to you or using another individual's District authorized accounts, user-id and/or passwords. Specific exceptions are allowed for HCBOE Technology personnel for authorized system operations and maintenance.
10. Adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the network infrastructure. This includes but not limited to, laptops, desktop computers and tablets.
11. Allowing non-district persons permission to use District assigned information systems on District equipment taken off-site.
12. Sharing the password of their unique HCBOE user ID or using this password to access other 3rd party web sites or applications.
13. The use of any "hacking tools" that can be used for "computer hacking" may not be possessed on school property, on any District premise, or run or loaded on any District system.

B. Sensitive Information

HCBOE employees who have or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and other applicable laws and regulations, as they relate to the release of student information.

1. Employees may not disclose sensitive or personally identifiable information regarding students or staff to individuals and/or parties not authorized to receive it. Authorization to disclose information of a student to individuals and/or parties must strictly adhere to regulations set forth in the FERPA
2. Information contained in these records must be securely handled and stored according to HCBOE directives, rules and policies and if necessary destroyed in accordance with state information retention standards and archival policy.

C. Granting Access to Secure Locations

Staff members may only grant access to sensitive and secure areas, including but not limited to, server rooms and wire closets, after verification with **Technology** of the credentials and need for access of the person requesting access.

D. Limited Personal Use

HCBOE does not grant any ownership, privacy or an expectation of privacy in the contents of any message, including email, or other Internet activities involving HCBOE resources or equipment.

Personal use is prohibited if:

1. It interferes with the use of IT resources by the District;
2. Such use burdens the District with additional costs;
3. Such use interferes with the staff member's employment duties or other obligations to the District; or
4. Such use includes any activity that is prohibited under any district (including this rule), board policy, or state or federal law.

E. Email Maintenance

Each District e-mail user is responsible for the content of all text, audio, or image that he or she places or sends over the Internet or District email systems.

1. Email messages are considered public records

F. Personal Devices

1. I will not post on any social media sites, take photos or record video of any student, teacher or administrator unless I have that individual's express permission to do so.
2. I understand that the district is not responsible for theft, damage or loss of my personal devices.
3. I understand the Technology staff cannot assist me with my personal device (such as but not limited to; phones, laptops, tablets) including setting up email and connecting to other district accounts on that device.

G. Consequences

Employees who violate this administrative rule may be subject to discipline, including up to termination. All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to an employee's supervisor and directly to the Help Desk. Suspected criminal activity must be immediately reported to law enforcement.

I have read and agree to the terms of the districts Acceptable Use Policy.

Print Employee's Name: _____ School: _____

Employee's Signature: _____Date:_____