ACCEPTABLE USE POLICY

By using EPS services, all individuals, including, but not limited to, employees, students, customers, volunteers, and third parties, unconditionally accept the terms of this policy.

Acceptable use of EPS information technology resources is based on common sense, decency, ethical use, civility, and security applied to the computing environment. All authorized users may expect reasonable privacy with regard to all computer files and e-mail. The school district may access district-owned or networked computers for maintenance and upgrades and to monitor or troubleshoot networks for related security, network audits, investigations, and/or legal requirements. Computers or systems may also be accessed through established procedures for reasonably suspected abuse of this policy and/or other district acceptable use policies. If illicit activity of any kind is suspected as a result of routine monitoring, an internal or external investigation may result. Users may be entitled to notification of such access, and, whenever possible, notification should precede access. Any actions that compromise the integrity of the district, data facilities, networks, services, or resources is strictly prohibited. Examples of unacceptable uses include, but are not limited to, the following:

1. Using the resources for any purpose which violates federal or state laws.

2. Using the resources for commercial, sales, and advertising purposes without district approval.

3. Using excessive data storage or network bandwidth in activities such as the propagating of "chain letters" or "broadcasting" inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages.

4. Sending or storing for retrieval patently harassing, intimidating, or abusive material.

5. Misrepresenting your identity or affiliation while using information technology resources.

6. Using someone else's identity and password for access to information technology resources, logging others into the network to access information technology resources, or using the network to make unauthorized entry to other computational, information, or communications devices or resources.

7. Accessing material that, in EPS evaluation, is obscene, defamatory, or constitutes a threat, including pornographic material.

8. Attempting to evade, disable, or "crack" passwords or other security provisions of systems on the network.

9. Reproducing and/or distributing material protected by copyright, trademark, trade secret, or other intellectual property without appropriate authorization.

10. Copying or modifying files belonging to others or to the university without authorization, including altering data, introducing or propagating viruses or worms, or simply damaging files.

11. Using the resources for political activities, including organizing or participating in any political meeting, rally, demonstration, soliciting contributions or votes, distributing material, surveying or polling for information connected to a political campaign, completing political surveys or polling information, and any other activities prohibited under the ethics act and/or other state/federal laws.

12. Purposefully interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment.

13. Use of personal social media sites, following specific direction to cease or not utilize district equipment or time to an extent or during time periods that would interfere with professional responsibilities, including, but not limited to, Facebook, Twitter, Flickr, Pinterest, LinkedIn, Foursquare, etc., unless associated with professional responsibilities.

14. Intercepting or altering network packets.

Certain violations of this acceptable use policy, which involve the potential for illegal conduct (including accessing certain pornographic sites or any activity which may constitute fraud or the misappropriation of district resources), may be reported to external agencies or law enforcement for investigation.

Access to the information technology environment at Eufaula Public Schools is a privilege and must be treated as such by all users of these systems. Like any other campus facility, abuse of these privileges can be a matter of legal action or official campus disciplinary procedures, up to and including termination.

Depending on the seriousness of an offense, violation of the policy can result in penalties ranging from reprimand, loss of access, or referral to authorities for disciplinary or legal action. In a case where unacceptable use severely impacts performance or security, in order to sustain reasonable performance and security, Information Technology Services will immediately suspend an individual's access privileges.

July, 2014