

WAYNE COUNTY BOARD OF EDUCATION POLICY MANUALSection 3000 – Educational ProgramPolicy Code: 3225 Technology Responsible Use

not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy [4705](#), Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school system websites or web pages or elsewhere on the Internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy [4700](#), Student Records. Users also may not forward or post personal communications without the author's prior consent.

9. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school system technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.

10. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or other Superintendent designee.

11. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

12. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.

13. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.

14. Employees shall not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

15. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security

