

INTERNET ACCESS POLICY FOR STAFF

Employees of the Deposit Central School District will be issued a password and e-mail address for use on the District's internal network and computers. The password and e-mail address will also allow the individual user to remotely access the District network from external locations. Employees should be aware that District computer use is limited to activities supporting the educational mission of the District. With that in mind, District internet resources shall not be used for:

- Leisure time activities such as personal correspondence, recreational reading, game playing, or other activities.
- Commercial activities, online shopping, online auctions, purchases, sale of goods, and sale of services.

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The computer coordinator may access all such files and communications to ensure system integrity and compliance with requirements of this policy. Staff should NOT expect that information stored on the DCS system will be private.

Staff members who engage in unacceptable use may lose access to the DCS system and may be subject to discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the district.

Employees must work to preserve the efficient operation of the District's computer resources. No holder of any password or e-mail account within the Deposit Central School District may load software including free-ware or share-ware not licensed to the District on any District computer resources. No peripherals such as printers or storage devices may be connected to District computer resources unless they are the property of the Deposit Central School District. No computers other than those belonging to the District may be connected to the District's network unless given permission to do so by Administration or the IT staff.

Employees will adhere to the following guidelines which are consistent with our workplace standards on harassment, student relationships, conduct, professional communication and confidentiality.

- An employee shall not make statements that would violate any of the School's policies including its policies concerning harassment or discrimination. An employee may not disclose any confidential information of the school or confidential information obtained during the course of his/her employment, about any individuals or organizations, including students and/or their families. Employees shall exercise good judgment on content that is shared on social networks/media or through any other method of communication. (i.e., texting e-mails).
- District employees are strongly encouraged to carefully review the privacy setting on any social media/networking sites used.
- Exercise care and good judgment when posting content and information to such sites. When using a social media site, employees are strongly discouraged to include current students as friends and or followers.

The above policy was adopted 4/16/2012.