Office of Information Technologies

Information Technology Procedures and Best Practices

The purpose of this document is to provide answers to questions that are frequently received in the IT Department relating to backing up data stored on end-user systems, managing e-mail and passwords, requesting technical support, and IT-related purchases.

1. **Backing Up**
   a. It is important that all staff members take responsibility for backing up their critical documents on a regular basis. Using the Backup Docs program in conjunction with the STAFF1 server is the preferred method of backing up because it allows staff members to store their documents in a secure location on the network.
   b. Avoid the use of removable media (CDs, DVDs, Thumb drives, etc.) for backing up confidential information, as these media can easily be misplaced.
   c. If a staff member's computer needs to be reimaged, the staff member is responsible for restoring items from their backup.
   d. Anyone who would like training on the use of the Backup Docs program or who wishes to use another backup strategy should contact a Technology Integration Specialist for assistance.

2. **E-Mail**
   a. All staff members are reminded that the use of the BASD E-mail system is for professional, job-related communications and responsibilities. Chain letters, jokes, and other non-work related items are not permitted. Please refer to the guidelines in the Acceptable Use Policy for more information.
   b. There are SPAM filters in place for catching junk mail; however, no SPAM filter is 100% effective. Hackers frequently make attempts to deceive users into supplying passwords, and credit card or bank account information. Other scams may ask to respond to unclaimed lottery winnings or requests for emergency loans, approve a Youtube video, or to enter credentials for an webmail account. At first glance, some of these messages may appear to be legitimate. Staff members are advised to delete these messages and not respond to requests to validate accounts or supply personal information, including passwords. The BASD IT department will never ask staff members to send a password or validate an account through e-mail.
   c. Staff members are advised not to open attachments in SPAM e-mail messages, and not to click on links within SPAM e-mail messages, as

these are often infected with viruses or connected to malicious web sites that can compromise the security of the district's computer systems.

3. **Passwords**
   a. BASD Passwords are to be treated as <u>confidential</u> information at all times because they are used to protect access to district e-mail and district IT systems.
   b. **Passwords for e-mail and other district systems are not be shared with substitutes, students, or colleagues.** If a substitute needs access to a system, or if e-mail needs to be forwarded or redirected, staff members should contact their immediate supervisor, who will make the necessary arrangements with the IT Department.
   c. Passwords should not be kept on post-it notes, saved in web browser login screens, or stored in other visible locations.
   d. If anyone suspects that their password has been compromised, they must immediately inform their supervisor and contact the IT Department (Ext. 35971) to have it changed.
   e. System passwords will be changed on a regular basis. The next password change will take place in Fall 2012.

4. **Technology Work Order System**
   a. The Technology Work Order System is the preferred method of contacting IT for technical support requests. The work order system is located at http://www.beth.k12.pa.us/workorder/. By using this system, all requests are organized and prioritized so that the support technologists and technical assistants can respond efficiently. If there is an emergency and immediate technical assistance is needed, staff members may call the building technical support office or call the IT office at Ext. 35971.
   b. When entering a technology work order, staff members should provide as much detail as possible, including symptoms and steps that can be taken to re-create the problem. Please make use of the BASD Tag/Barcode number whenever possible.

5. **IT Equipment**
   a. All staff members are reminded that district-owned IT equipment and software is to be purchased through the IT office, whether it is being purchased with district funds, PTO/PTA funds, student activity funds, or grant funds. This applies to computers, printers, cameras, data projectors, and other hardware peripherally connected to computer systems. This is done to insure compatibility with other district equipment and to maximize the savings provided by state pricing contracts. The Technology Integration Specialist will be the first point of contact for researching products and obtaining price quotations for classroom technology equipment and software.

b. Equipment that is the personal property of a staff member is not supported, and the IT department assumes no responsibility for its compatibility with other systems.

6. **District-owned Software**
   a. Staff members are not permitted to install personally-purchased software, including music, onto district-owned equipment, and the IT department assumes no role in supporting it.   Requests to purchase software should be approved by the building administrator, and previewed/tested by the IT department before the purchase is made.   If district-owned equipment needs to be reimaged or moved to another location, the IT department takes no responsibility for reinstalling or recovering unauthorized software.
   b. The preferred productivity software tools for word processing, spreadsheets, and presentations are Word, Excel, Powerpoint, Pages, Numbers, and Keynote.
   c. Appleworks was discontinued by Apple in 2007 and is no longer being supported. Any staff members who are still using Appleworks are advised to convert documents to a newer format as soon as possible. New software images for students and staff will not include Appleworks.
   d. Pending final budget approval, updated versions of Word, Excel, and Powerpoint will be deployed in the 2012-13 school year. Training will be scheduled for staff.
   e. During the remainder of the 2011-12 school year and into the 2012-13 school year, operating systems on the teachers' Macbook Pro laptops will be upgraded from OS 10.5 to OS 10.6.