User Guide Table of Contents

Introduction

The purpose of this guide is to provide all users with a document that describes the district's data network, the policies that govern user access to the network, and how to create, save, and recover documents on the network. It should be recognized that this guide is written from a district perspective and, as a result, it is generic in nature. There may be building specific issues that are not covered in this guide.

Network Philosophy

While our network is, technically, a data network, its intended use is to support the delivery and management of instruction. We must also make sure that our network is safe, secure, stable, reliable, and predictable.

The one document that drives most of our decisions is the District Technology Plan. This document was originally adopted in July 1999, revised most recently in 2022. A new plan was developed in 2021-22 through the efforts of the Technology Planning Committee. You can access the 2022-25 Technology Plan through the District Technology web page. It is a live document that is constantly under scrutiny and revised on a yearly basis to reflect changes in technology, curriculum, regulation, funding and many other outside factors. The District TechnologyPlanning Committee meets regularly to review and revise the plan.

Our challenge is to make sure that all the hardware and software works and is appropriate for the instructional or instructional management use to which it is applied. In the end, we are not just acquiring technology; we are acquiring technology that meets our instructional and instructional management needs as described in the currently approved Technology Plan. Additionally, this technology must be supported with the training and logistics needed to ensure that it is used appropriately by all users.

Brief Description of the Baldwinsville Data Network

Following are some statistics that describe and give dimension to the Baldwinsville network.

Users	7,000 (6,000 students, 1,000 staff)
PCs	1,770
iPads	900+
Chromebooks	6000+
Aruba switched network	40 Gbps between buildings, 10 Gbps within
Aruba wireless network	802.11a/b/g/n/ac duel band

In addition to replacing computers this year, we take advantage of technology that allows us to save files directly to the "Cloud". Google Drive allows us to keep our in-house storage costs down. The amount of data that we manage is expanding exponentially. In order to save cost, we place limits on most users personal "H:" drive. Please remember that storage space is costly and finite. All users are encouraged to, at least once a year, review the content of their "H:" drive deleting any obsolete, duplicate, or unnecessary data. It should be noted that all student data is deleted at the end of each year.

Each network user belongs to a group that has a particular set of rights and privileges associated with their anticipated needs. These rights and privileges can change, subject to need and a review by the building administrator and District Technology staff. User access is safely and securely managed through a unique combination of user names and passwords with the passwords being changed at least every 60 days.

To insure the safety and security of user data, it is very important that users maintain the security of their personal password!

We operate a virus detection package on the network that will scan all files, including e-mail attachments, for computer viruses. It is important for users to be sure of the source of a file before they open it. If any user is unsure of the status of a file, they should not open it until they can confirm that it has been scanned for viruses.

We continue to look for ways to reduce printing and the number of printers.
We will monitor each printer and report out data as far as usage, repair status and toner levels. Our aim is to have the right printer for the job.

District's Acceptable Use Policy (AUP)

An Acceptable Use Policy (AUP) is an approved document that describes the current policies regarding the acceptable use of district networked and standalone hardware and software and other technology owned or subscribed to by the district. A controlled copy of this, and all policies, is available on the District website. See the Reference Documents and Forms section of this guide for a current copy of the district's AUP.

This policy also includes a very specific listing of appropriate user behaviors that apply to all student and staff users of district network resources. Other district and building specific regulations flow from this policy. It is important for all users to review and understand this policy and any regulations that apply to their work location.

Following is a list of specific system use requirements that apply to all users of system wide networked resources regardless of building, platform, operating system, and application.

1. Only District Technology staff is authorized to make hardware or software configuration changes to any district owned network connected or standalone resources. These changes include:
    - The installation or de-installation of software applications.
    - The installation or de-installation of standalone or networked hardware.
    - The removal, relocation, addition, or reconfiguration of any hardware.
2. New software installations (including downloads) will not be made until the proposed software:
    - has been recommended by content area experts.
    - is approved by District Technology staff for network compatibility.
    - is previewed by content area experts and District Technology staff.
    - is funded to support the proposed level of installation, licensing, and required technical and user support.
3. Subject to the software review process, applications and other executable files may be installed on the server or workstation hard drive. Once installed, they will not be removed without additional software review.
4. The District Technology staff will identify network software, hardware, and other devices that will be supported district wide. This list will be updated and published as necessary. Other software and hardware may be installed, subject to the software and hardware review and approval process; however, it may not be supported by District Technology staff. In this case, outside technical and user support must be included in the funding of the purchase.
5. Users will be assigned network home (H:) directories in which to store files created on the District system. These directories will be limited in size subject to the nature of their use. Staff will also be issued a Google Drive. These are the

only locations where users should store data that they expect to be backed up by District Technology Staff.

6. Files (including e-mail) created and stored on the District system are subject to review by authorized District staff. These documents may also be subject to access as a result of formal Freedom of Information Law (FOIL), requests and other legally enforceable access requests.
7. Unauthorized access to any part of the District system is strictly prohibited and may result in the loss of system privileges, District-imposed discipline, or legal action.
8. Unless specifically authorized and enabled by District Technology staff, no data will be stored on a general use workstation hard drive (drive C:). Generally, data should be stored on the user's server-based home (H:) directory or on the users Google drive which is backed up. Only the files stored on District servers may be backed up by District Technology staff. Since storage space on the network H: drive is limited, users will be required to purge their files on a regular basis. With notice, District Technology staff may also remove or store to disc large files, especially video and audio data.
9. Generally, data can be read to and accessed from the workstation, CD, DVD, thumb or other drive. Since some of these storage devices are a ready source of viruses, we may disable this access on a public access machine if it represents a virus threat.
10. Users will not access computer games from any source unless used as a part of teacher supervised instruction or activity authorized by the building principal.
11. Only screen savers and wallpaper included in the current workstation operating system can be installed on the desktop. Unauthorized screen savers and wallpaper will be removed from any workstation before any maintenance or troubleshooting work is done on it.
12. Student and staff access to the District network for any purpose will be password controlled.
13. No executable files in any form will be downloaded from the Internet or other outside sources or installed or stored on any District resources other than by District Technology staff. This restriction includes Hotmail, AOL mail, Instant Messaging or any other commercial, privately developed, locally developed, or experimental executable file, macro, or application.
14. The district will maintain student E-MAIL accounts for the purpose of accessing Google Drive and Apps. The District will make E-MAIL accounts available to staff. Use of E-MAIL will be limited to that which is available through the district point of presence (POP), which does not allow nor support Hotmail. The use of any district supplied E-MAIL account will be strictly limited to communication in support of the instructional, non-instructional, and administrative work of the district. Since all students do not have equal access to technology outside of school, the instructional application of electronic resources will be supplemental to, and not in lieu of, other district supplied instructional resources.

15. All users of the District system are specifically prohibited from engaging in the following activities on district owned resources:

    - Sending or displaying offensive messages or pictures: pornography, etc.
    - Using obscene language.
    - Harassing, insulting or attacking others.
    - Damaging computers, systems or networks.
    - Downloading or installing unapproved software or hardware.
    - Violating copyright laws and the valid licensed rights of others.
    - Using another user's password.
    - Encrypting or password protecting material stored on the system.
    - Possessing programs used for hacking or stealing passwords.
    - Trespassing in another user's folders, work or files.
    - Intentionally wasting limited resources.
    - Employing the network for non-school related, commercial or other private purposes.
    - Use of an account by anyone other than the account holder.
    - Requesting unnecessary and lengthy material that ties up system resources.
    - Sharing of Staff or Student PII with unauthorized individuals or vendors.
    - Email, meeting and document storage are to be used for District business only

Implementation of the District's AUP

It is important that all users have the opportunity to review, ask questions about, and understand the AUP which is part of the yearly training sequence. Any changes made since then have and will continue to be distributed via this document as it is revised each year. New staff will have the opportunity to review this document and ask questions about its content during new staff orientation. If at any time you have questions or concerns about the AUP, please feel free to contact the Director of Technology.

Each building should develop their own strategy for reviewing the AUP with students. Generally, it is included in the student handbook for the secondary buildings and discussed in the library for all K-5 buildings. It is very important that this review be done each year during the opening weeks of school, as some of the behaviors described above are not intuitive. As a result, without this review opportunity, a user could honestly say that they were not aware that their behavior was a misuse of the data network or other district resources.

Keystroke and Email Monitoring

Per the District Acceptable Use Policy, all data created on the district data network belongs to the district and can be reviewed by District Technology staff. While possible, this rarely happens and would only happen as a result of concerns raised for other reasons. We do run a keystroke monitor that is designed to look for keystroke combinations that can, in the right context, indicate a concern for possible abuse or at least misuse of the District data network. Reports generated by this monitor are reviewed and, subject to the nature of the report, appropriate action is taken.

All email is archived in a way so that it can be easily searched and retrieved should it be necessary in response to a FOIL or other legal request.

AristotleK12 Content Filter

AristotleK12 Content Filter is an Internet content filtration application that is applied to any content that we receive from our Internet service provider. We, like all schools, are required by law, regulation, and Board policy to take electronic measures to ensure that the content available in any instructional building is free of material that is locally defined as objectionable. Subject to an approval process, sites can be blocked or unblocked. See the Reference Documents and Forms section of this guide for an example of the Content Filtration Block/Unblock Form. Copies of this form are available in your building's main office.

The laws, regulations, and policies regarding content filtration require that the filter be applied to all technology assets. If a workstation reaches the Internet through some ISP other than the BOCES, we must apply a locally configured filter.

Wireless Networks

Beginning in 2012, the BCSD began to provide wireless networks in District buildings. As of this latest revision, all buildings have a bifurcated wireless network which consists of a "Guest" and a "Private" network.

Guest Network

All privately-owned wireless devices will connect to this network. The Guest network is available for school-related purposes and does not require a log in. This network is limited to a fully-filtered connection to the public internet through BOCES. There is no access to District technology resources including the storage area network.

Private Network

District-owned wireless devices may connect to this network. This network requires a secure password and a login through the AristotleK12 Content Filter. Access to District technology resources is available through this wireless network. Access to this network must be approved by the Director of Technology.

Account Management, Group Descriptions and Available Resources

All new staff members and students will have a network account created at the time that they formally enter the district. All new staff members may have an e-mail account. These accounts are enabled, maintained and disabled by District Technology staff. We are generally, but not always, aware of new staff entering the district or current staff moving from one building to another. Since it takes several days to create an account, new users should check with District Technology to make sure that their accounts are active when they need them. We do a batch import of student names during the summer to create student accounts. The need for new student accounts in the buildings should be sent to the help desk. All account maintenance requests (changes in user access, password changes, file access etc.), should be sent to the Help Desk.

Employee account creation and maintenance tasks are managed through the use of The Employee Network and E-Mail Account Request and Change Form. See the Reference Documents and Forms section of this guide for a copy of this form.

When a user leaves the district or transfers to a new job, their account typically is disabled immediately unless other arrangements are made. If a user transfers from one job location to another, it is important to let District Technology know this fact so that proper file access is maintained. This is especially the case when the need is for a user to have access to data saved on another user's "H:" drive. This access will only be enabled after the building principals in both buildings agree that this access is necessary and a formal approval e-mail is sent to the Director of Technology. Disabling student access is done on a yearly basis unless specifically requested by the building principal.

Subject to "H:" drive size limitations, employee data will be maintained from one year to the next. Student data is deleted from the "H:" drive at the end of the school year. Student data can be saved on removable storage or a "cloud" account. Accounts that have been inactive for more than 90 days will be disabled. They can be enabled by sending a formal request to the Help Desk.

Once their account is created, each user will be placed into a group. Examples of groups include:

- Students by grade
- Teachers by grade and building
- Building office staff
- Administrators
- DO Staff
- Librarians
- Custodians
- Nurses

Each group and, by their membership in a group, each user, will be given access to the resources assigned to their group. From time-to-time it may be necessary to give a user temporary or permanent access to or denial from other resources. This is accomplished through moving a user to another group, creating a new group, or modifying the access of an existing group.

Each user will sign on to the network through a login screen using a user unique combination of their user name and password. Staff user names will typically be the user's first initial and last name. Where two or more people have the same first initial and last name, they will be differentiated by an additional character that will make their user name unique. Staff will, initially, be issued a temporary password and then will be required to establish their own permanent password. Student user names are a combination of the last two digits of their graduation year, then the first three letters of their last name and then the first three letters of their first name. Students will be issued system generated passwords. District Technology staff will supply the building librarian and, in the case of the elementary buildings, the classroom teacher and lab TA, with a list of student passwords should there be the need to "remind" a student user of what his or her password is.

If a staff user forgets their password, they must log their request for a new password with the Help Desk at helpdesk@bville.org or call 638-6190. The new password will be sent to them via interoffice mail. Please note that you have only six login attempts before the temporary password becomes disabled. If a staff member wants to change their password, and they know their current password, they can key in Crtl, Alt, Delete all at once and follow the screen prompts. All user accounts are reset each year with a new password.

To insure the safety and security of user data, it is very important that a user maintain the security of their personal password!

The Software Center

In the past, most workstations in the classrooms and all building libraries and offices opened with a Windows desktop. This desktop includes a variety of application and other icons as well as access to the start bar. The application icons available to users in the Software Center will depend upon the rights granted to the user. Most PC users receive a modified Windows desktop. This is the same desktop that you might see on your windows machine at home. Some of the windows desktop functionality may be removed so that we can manage the computer in our network environment.

How to Log on to the Network

Logging on to the network is as simple as powering up the workstation, if it isn't already powered up, and following the screen prompts that appear. The first screen that you see will display the following certification.

By logging on to this system, you agree to abide by the Acceptable Use Policy of the Baldwinsville Central School District.

By clicking OK, a user is certifying that their use of the network will be in accordance with the District's AUP.

How to Access a PC Based Application and Create a Document

Whether launched from the Software Center or the Windows desktop, an application is launched by clicking on the correct icon. Once launched, the application can be used to create documents and other application specific files per the instructions unique to the particular application that is launched. This process is independent of the method by which the application was launched.

How to Save a Document or File

All users will be assigned a limited amount of server-based storage space. This space is called their "Home Directory" and the drive will be referred to as the "H:" Drive. The "H:" Drive can also be accessed via the "My Documents" icon. All documents that are saved will be automatically saved to this drive. You will be prompted through an application unique "save as" box to give the file a name and, if it exists, identify a particular folder in which to place the file. If a folder is not identified, the file will be placed directly into the user's "H:" Drive. Some users may also be able to save to other drives beside the "H:" Drive; however, this will be a manual process.

Users are discouraged, and in most cases prevented, from saving to their "C:" Drive, as the "C:" Drive can be corrupted and it will be completely erased once a year during the annual re-imaging process or more often for maintenance purposes. If this is necessary, it is very important that the user and technician doing the re-imaging identify and manually back up any data that is not also on the user's "H;" Drive. Locally installed applications not included on the image to be installed should also be identified at this time so that the technician can reinstall them after the re-imaging process is completed.

Users are encouraged to develop strategies that organize their files and folders in such a way that they can be found again later. There is no one right way to organize files and folders. These strategies are, typically, a result of experience and personal preference. District Technology staff are available to help users develop these strategies.

Users are also encouraged to use Google Apps and Drive to store files. This method of storage and file creation off many more opportunities for collaboration and are device-agnostic. Files stored in Google Drive are accessible anytime from anywhere on almost any device with an internet connection.

How to Find and Open an Existing PC Document or File

Typically, a file or folder can be found where the user left it. This sounds obvious and easy, but it sometimes is not, as it requires that the user remembers the name of the file or folder and its location. Again, there is no one right way to save files and folders, and the way that they are saved will determine where to find them. Once found, reopening the file or folder can be accomplished by simply double clicking on the icon associated with the file or folder. If you click on a file, the application that it is associated with will automatically be launched if the application is installed and the user has rights to the associated application. Occasionally, the associated application will not auto launch. Typically, this is due to the fact that the application is not installed or the file is not associated with the application. In this case, open the application first and then open the file from the application document launcher.

Internet Enabled Resource Use Guide

This section is intended to define acceptable student and staff use of any district Internet enabled resources to include e-mail, web content browsing, and website or webpage creation.

E-mail

All district students in grades k-12 and staff may have a district-maintained e-mail (G-mail) account. Student provided email accounts will only communicate with other @bville.org email accounts and will not be used for anything purpose outside of instruction. Moving forward from the date of this publication, students will only be able to post their initials or their own picture when personalizing their remote learning applications (i.e. Gmail, Google Meet, Zoom, etc.). Staff provided email accounts will not be restricted. However, the purpose of this communication is to be professional in nature and support the business of the district.

The use of district provided e-mail accounts is to be in strict accordance with the district's Acceptable Use Policy and other Board policies. It is very important that e-mail content originating inside the district not contain staff or student personal information. At no time should a user respond to a solicitation for this information. Any solicitation of this nature should be forwarded to the Director of Technology.

Users will log (authenticate) into the e-mail browser with a screen name and password. As of August 1, 2022, all staff will be required to enable multifactor authentication on their Google mail accounts. Instructions for setting this up are available on the District Technology website or call the helpdesk. This authentication screen will also provide access to the district e-mail user directory. Subsequent screens will provide the typical e-mail control features found in most e-mail software applications. All e-mail files are saved and backed up. This allows users to access their e-mail history from any networked workstation. Users may be required, from time-to-time, to delete older information if their files become too large.

Content Browsing

Internet content is browsed via Chrome, Firefox, and in limited cases Safari. By default, the browser will then open the district homepage (www.bville.org).

In accordance with the District Acceptable Use Policy, users are free to browse Internet content subject to any content filtration applied to the search results. **Differing filtration profiles are established for faculty, staff and students**. It is our intent to provide staff with the rich instructional content that is available on the Internet; therefore, faculty and

staff in the district will have minimum filtration of Internet resources. The filter will block known security issues, pornography and websites that require large amounts of bandwidth (i.e. internet radio stations). Students however, will have a much more aggressive filter applied. Block and unblock requests must be made in accordance with the district Acceptable Use Policy and administered via the "request review" feature in Aristotle or a helpdesk request ticket. It should be remembered that currently any block or unblock action taken in response to a request will affect the entire district and this fact is considered before the request is approved.

All users must be mindful of the copyright and licensing restrictions that apply to content available on the Internet. The fact that you can copy content does not mean that you should, especially if your intent is to incorporate this content into a piece of work for which you intend to take credit and/or duplicate. You should review any concerns you have about the appropriate use of electronic content with your building library media specialist.

The downloading and installation of any executables from any source including the Internet is absolutely prohibited and will be treated as a severe violation of the district AUP.

Website Creation

The district continues to expanded its website. While hosted at the BOCES, the website is staffed by a district webmaster and a webmaster in each building. All webmasters are responsible for training, administering building web pages, and helping users post appropriate content to their building web pages. Each teacher has the ability to create their own instructional page(s) to be used in whatever fashion is appropriate for their instructional needs and in the context of their building's on-line personality. It is important that the design of any page follow the Board approved website creation policy. This policy includes the requirement that all district website content be in accordance not only with the AUP, but also various laws, regulations and other policies that govern the creation of a school district website.

BOCES Services

The district purchases many technology-based services from the OCM BOCES. They include SchoolTool, WINCAP, Nutrikids, and IEP/AIS Direct support. Most of these services share a common SIS database that is housed at the CNYRIC. Access to these services is either password protected, if web based, or based on a user profile. Requests to add or change access should be sent to the District Technology department via helpdesk@bville.org or by calling 638-6190.

Hardware and Software Changes

It is very important that hardware and software changes be managed in a way that insures that they support the instructional goals of the district, can be implemented and be managed by District Technology personnel, do not create a licensing violation, and are supported within the approved budget. The District AUP addresses these requirements; however, their implementation is described in the hardware and software change procedure that is a part of the Reference Documents and Forms section of this guide.

Use of District Assets

We are required by regulation and good management practice to keep a very close control over the use of district assets. This is especially true of assets that are removed from within the physical boundaries of the district. Assets may only be loaned to District employees.

As a general rule, we do not loan the use of any networked or standalone desktop equipment, as the potential for damage and the work involved in reconfiguring them is too great to justify such a practice. We do have a couple of laptops that can, with at least two weeks notice, be loaned, subject to the approval of the building principal responsible for the activity. Examples of appropriate use include Board, PTA, association and off-site professional presentations, curriculum work and training. We are not able to loan software other than that which is installed on loaned laptops.

AV equipment, to include but not limited to digital cameras and video projectors, falls under the same Use of District Assets Policy as computer hardware and software.

The management of these assets is more fully described in the Assets Use Request Procedure that is a part of the Reference Documents and Forms section of this guide.

All district assets are inventoried. They should have a district asset tag securely applied to them that is used to track them and maintain inventory and lifecycle event records. If any student or staff brings personal equipment into a building for any length of time, it should be identified as personal equipment so that it does not get inadvertently included in the district asset inventory.

Hardware Disposal and Redeployment

As time passes, equipment will become obsolete, unable to support its current application, impossible to repair, or too expensive to repair. In some cases, we can reconfigure equipment and re-deploy it to a more general application with lower resource requirements. Eventually, equipment is no longer able to support our needs and will be discarded. This is not as simple as just throwing it away. To start with, computers and many computer peripherals are considered hazardous waste. As a result of this classification, we must apply the same disposal practices as we would to other similar forms of hazardous waste. Regardless of what it is, no district asset can be disposed of until the Board approves it.

The management of the disposal and re-deployment process is more fully described in the Computer Equipment Disposal Procedure and Non-Computer Equipment Disposal Procedure both of which are a part of the Reference Documents and Forms section of this guide.

District Technology Contacts

The following table is a function list of District Technology Staff.

Contact	Title	Phone/E-mail	Contact For
Linda Moehringer	Data Center Helpdesk Operator/AV Clerk	638-6190 helpdesk@bville.org lmoehringer@bville.org	to initiate a service call, lamination (Grades 6-12), reserve AV equipment, document scanning
Tom Liggett	Network Administrator	tliggett@bville.org	general network administration, X-Stop, new/revised user accounts, server and connectivity issues
Mike Lasinski	Network Technician	mlasinski@bville.org	general hardware and software installation and other service issues
Jim Froio	Network Technician	jfroio@bville.org	general hardware and software installation and other service issues
Alex Bateman	Network Technician	abateman@bville.org	general hardware and software installation and other service issues
R.J. DeLisle	Director of Technology	638-6103 rdelisle@bville.org	All questions

Please note that **ALL** requests for service must go through the helpdesk. Any call made directly to any of the staff named above, with the exception of Linda Moehringer, will be redirected to Linda. The purpose of the helpdesk is to summarize and manage our calls and to ensure that they are responded to in a priority order. From this data, we are also able to generate reports that help us make good decisions about how we manage our equipment. User's may also enter help requests via the Baldwinsville website: Staff only: Technology Help Desk. (http://www.bville.org/reqform.cfm)

Supported Applications

Over the years, a number of different applications have been installed on PCs throughout the district. In most cases, a finite number of installation licenses were purchased for these applications. It is very important that we maintain control of our software installations. The district does not allow the installation of software on district hardware for which we cannot produce a valid current license. If there is any question regarding the validity of an installation, the application will be de-installed. The AUP requires that no software be installed until it has been reviewed by District Technology staff. This includes the downloading and installation of executable files from the Internet or any other source of electronic media.

The AUP clearly covers the process by which an application should be reviewed and approved for installation. The fact that it is approved for installation does not necessarily mean that District Technology Staff can support it once it is installed. If this is the case, the purchaser must include tech support in their purchase of applications that cannot be supported by District Technology staff. The process by which software is installed or de-installed is more fully described in the HW and SW Change Procedure that is a part of the Reference Documents and Forms section of this guide.

The installation of all other applications must be reviewed and approved first by District Technology staff. The requester must provide District Technology Staff with the installation media and a license before the software will be installed. Maintaining the license and media will be the responsibility of the requester.

Access to programs or websites requiring personal identifiable information (PII) is prohibited until a reviewed Data Privacy Agreement (DPA) is in place with the vendor.

Safety and Security

A crucial element in the design and implementation of networked services is the maintenance of a safe and secure network. These needs grow out of good network management practices as well several laws that are unique to schools. All networks are subject to a variety of electronic threats. Some impact the electronic health of the network and the equipment on it. Others can impact the security of users, especially children. By law we are required to enact electronic measures to filter Internet content made available to children over the network. Our current filter can differentiate users and, as a result, faculty and staff will have access to many more Internet resources than students and therefore, must take measures to provide appropriate content for students. **Do not leave your workstation unattended while logged-in.** Lock your workstation or log-out. We are also required to maintain security on all personal information available over the network. These requirements have led to the log-in requirements described earlier in this document. The responsibility for maintaining the safety and security of users extends to all users and it is the origin of many of the user-based requirements described in the District Acceptable Use Policy.

One element of network safety and security that is always a challenge is the elimination of various electronic threats such as viruses, worms, and Trojan horses. Less of a threat, but still a potential thief of network resources, are spam, pop ups, and other annoyances.

We maintain a very sophisticated firewall and antivirus protection protocol on our network to prevent outside threats from entering. We can't however, prevent them once they are allowed inside our network. The practice of connecting non-district owned equipment to our wired network is not allowed without District Technology permission.

In summary:

- No equipment is to be connected to the hard-wired data network unless it is owned by the district and managed by District Technology Staff. The only exceptions will be presenters or vendors who must have temporary access to perform an authorized district function. Prior to connecting this equipment, it must be reviewed by District Technology staff to ensure that it does not contain potentially harmful files and that it is protected to the same level as district owned equipment is protected. It is the responsibility of the people sponsoring this activity to bring this need to the attention of District Technology staff in a timely manner. Since this review takes time, the request should be made at least a week prior to the date of need.

- District owned equipment that is used outside of the district or connected to other networks must be reviewed by District Technology staff before it is reconnected to the district network.

- Non-district owned wireless equipment must use the "Guest" wireless computer network, unless otherwise approved by the Superintendent.

Copyright

Per Board of Education policy 8350, we are required to abide by the provisions of the United States Copyright Law, (Title 17 United States Code Section 101 et seq.).

Just as with print media, there is the potential that users can violate copyright law in their use of electronic media. To help you understand your responsibility with respect to copyright, the district has purchased copies of Copyright: A Guide To Information and Resources 3rd Edition, by Gary Becker. This guide is available in your building library. We have also purchased the rights to post this guide on our intranet so that it can be accessed from within our network via a link placed on your building library website. Answers to questions regarding the use of any media and the possibility that this use may be a violation of Board policy or copyright law can be answered through a review of this guide or they can be directed to the library media specialist in your building.

Unsolicited Commercial E-Mail (SPAM) Filtering

Unsolicited Commercial E-Mail, also known as UCE or SPAM, presents a challenge to the District's IT staff. It is increasingly difficult to balance the need to protect e-mail users from the annoyance of inappropriate advertisements, scams, and e-mail borne viruses with the need to deliver appropriate e-mail messages in a timely fashion. As with any filter, there is always the possibility of "false positives" (an appropriate e-mail that is flagged as SPAM and not delivered) and, even worse, "false negatives" (a message that should be filtered but isn't). To meet these needs, we employ a filtering solution provided through BOCES.

Generally, our filtering (Mimecast) solution will require no action on your part. If you suspect that a particular message may have been improperly filtered you should contact the Helpdesk. Please be ready to provide as much information about the missing messages as you can, including the sender's e-mail address and the subject of the message. This information will be necessary so the District Technology can locate the message and take appropriate action.

Reference Documents and Forms

Attached are various current documents and forms referred to previously that apply to the management of district technology and network services. If you are viewing this document on-line, you can click on the document to go directly to it. These documents include:

Forms

- Internet Site Block Unblock Request Form
- AUP 8261: Staff Use of District Data Network Resources
- AUP Regulation 8261R: Specific District Wide Data Network Use Requirements
- AUP District System User Orientation Certification 8261F
- Internet Use Declination Form 8261F
- Computer Equipment Disposal Procedure
- Non-Computer Equipment Disposal Procedure
- General Equipment Disposal Request Form
- Assets Loan and Use Request Form
- Hardware and/or Software Change Procedure
- Hardware and Software Change Procedure and Request Form
- Employee Network and E-Mail Account Request and Change Form

Data Privacy

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Education Law 2-d and Part 121 of the Commissioner's Regulations outline requirements for school districts and BOCES related to the protection of the personally identifiable information (PII) of students, as well as some teacher and principal information. The law and the regulations require schools to undertake a multi-pronged approach to information governance.

Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. Examples include:

- Student name
- Parents' names
- Student address
- Student number
- Linkable information

Educational Agencies must ensure personally identifiable information is not included in public reports or other documents. Individuals with access to PII must maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody.

Do not store PII on removable hard drives, other transferrable media or personal devices.

ANNUAL EMPLOYEE TRAINING

Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Training should include training on the state and federal laws, and how employees can comply with such laws. You will be required to complete an annual training provided by the district.