School District of New Berlin

Bring Your Own Device Information

Students who choose to bring in their own internet-capable devices to any school in New Berlin will have access to the District wireless system. This document may answer some of the questions the community may have about this opportunity for students.

SDNB
Revised Fall, 2013

LL 9.2013

TABLE OF CONTENTS

PURPOSE/PLAN

In June, 2010, the State of Wisconsin approved our district's Information and Technology Plan. This plan outlines four goals that we believe are important to focus on in the area of instructional technology:

- Students will meaningfully apply technology skills to collaborate, create, innovate, and communicate.
- Through collaborative professional development, staff members will be connected learners who initiate and participate in global learning opportunities and applications for students.
- Stakeholders will benefit from consistent and reliable access to technology that will be used to expand learning and communication.
- The district will continue to build collaborative relationships to transform teaching and learning experiences for students, staff, families, and the community.

In continuing our efforts to these goals, we allow students to bring their own wireless mobile learning devices. This allows students to access our secure network with their own device within the school day through a common portal. This includes personal laptops, smart phones, and other handheld devices such as iPods and iPads.

While we are excited to offer this opportunity for our students and believe it will provide benefits in learning for students, we have developed guidelines in order to ensure that learning is the key focus and we promote the use of technology to enhance this experience for students and staff. As we support students, through their learning experiences, to take advantage of various online resources to collaborate, do their homework, access resources, etc., the BYOD program allows students to use their own device in a way that provides access to our system and filtered network while at school and continued access beyond the school day.

It is our expectation to provide ongoing training and support to staff members to better understand the possibilities that exist through students utilizing their own technology devices for learning, how to appropriately monitor and support the use of these devices, and provide information relative to utilizing the devices to expand the learning of students beyond the school day and classroom in ways not previously possible. We understand that this will continue to be a growth process for staff. Our goal is to give students access to learning tools as they benefit learning.

STUDENT QUESTIONS

+ *I have my laptop with me in class. How do I get on the Internet now?*

ANSWER: Most devices these days will automatically detect a wireless signal when one is within range. Most of the time, the device will "ask" you if you want to join the network. When prompted, choose "**SDNB GUEST**" from the list. Once you choose the network, you will be prompted to accept the terms of service/log in using your district ID and password.

+ *My laptop is not prompting me to choose a wireless network. Is there any other way to connect?*

Answer: In the settings menu of your device, there is usually an icon for a network, go to this icon and choose the SDNB Guest from the list or prompt your computer to look for wireless networks in range. Always consult your tool's owner's manual for exact directions for accessing a wireless network.

+ *I brought my iPad to school to use in the classroom, but my teacher said I couldn't use it in her classroom. Can I still use it?*

Answer: The teacher in the classroom is the final say on procedures in the classroom. If he or she asks you not to use your technology tool, then you should follow those directions. Access is only available, not guaranteed for each classroom situation.

+ *I just can't get my laptop to connect to the network. Can I get some help from someone?*

Answer: Resources may be available to help you connect to the SDNB Guest Network on campus; however, you will need to consult with school staff for these resources. It is not the responsibility of your teachers or other SDNB staff to troubleshoot individual devices during the school day, but they may direct students to the appropriate help available during lunch/study halls. It is suggested that students check their owner's manual for issues concerning connectivity.

+ *How do I save my work?*

Answer: You can save your work to your own device. Once you save your work, you can also upload work to your district home (H) drive through Stoneware. Please log into stoneware to find directions on how to do this.

🞣 *I need to print the something I just created, can I do this?*

Answer: Printing from personal devices is not available. Students are encouraged to email documents/projects, etc. to faculty & staff when appropriate in lieu of printing.

🞣 *My laptop was stolen when I brought it to school. Who should I contact about this?*

Answer: Bringing your own technology tools to school can be useful, however some risks are involved as well. It is always a good idea to record the device's serial number to have in case of theft. SDNB is not responsible for the theft of a device nor are we responsible for any damage done to the device while at school. Any time a theft occurs, you should contact a school administrator to make him/her aware of the offense.

🞣 *Why am I filtered on my own computer? Shouldn't I be able to see what I want to on my own tool?*

Answer: Student filtering is a requirement of all public schools. The Children's Internet Protection Act (CIPA) requires all network access to be filtered, regardless of the tool you use to access it while in a public school. Your laptop or tablet is the device to access web resources, but the network you are using while at school belongs to SDNB and will be filtered.

🞣 *Am I still held accountable for the Acceptable Use Policy I agreed to at the beginning of the school year even though this is my own personal computer?*

Answer: Yes. The Acceptable Use Policy for SDNB remains in effect even when you are using your own laptop, smart phone, iPad etc. Our policy is linked here:
http://www.nbexcellence.org/cms_files/resources/6155%20%20Policy.pdf

🞣 *Can I text in school?*

Answer:
At the secondary level, Students, during their scheduled lunch hour and in the cafeteria only, may use their devices as they wish (call/text/use headphones).   Use of cell phones in the hallways, between classes, or for any non-educational endeavor may result in the device being confiscated and given to the main office.
At the elementary level, students are not allowed to text during the school day.

🞣 *Can I take pictures or videos with my own device while at school?*

Answer: Pictures and videos are not allowed to be taken during the school day unless under the direct supervision of an adult for educational purposes.

🞣 *What can I use my laptop/device for during class?*

Answer: Students may use their device during class with the permission of their classroom teacher. Please understand that some teachers will allow devices to be used for a variety of reasons based on their classroom and the specific activity being done during a class. What is allowable one day may not be so the next. Based on this information, students are strongly encouraged to check with their individual classroom teachers for clarification on when and how to use their device(s).

STAFF

<div>+</div> *My classroom is not conducive to student owned technology, am I required to allow my students to access their technology tools in the classroom?*

Answer: No. Although we encourage teachers to leverage the student owned technology tools in their classroom for learning, there is no requirement of teachers to allow this. You are in charge of the way your class functions and the rules that apply.

<div>+</div> *Some of my students cannot access the network on their laptops or phones. I don't have time in a class period to help them with this. Should I put in a help request or call the help desk?*

Answer: No. Students who cannot access the guest network or who may have technical issues with their technology tool need to take care of this issue by working with their user's manual that came with the device outside of the classroom. These are not school-owned devices and the district will not be allocating resources at this time to troubleshoot issues. You are welcome to help if you choose, but it is not a staff member's responsibility to ensure that student owned technology is functioning properly.

<div>+</div> *I have students on my campus who are accessing the Internet using their provider's data plan (AT&T, Sprint, Verizon etc.) on their smart phones or laptops, hence bypassing the filter. Is this a violation of the student AUP?*

ANSWER: This is not an AUP violation because the student is not bypassing the filter on the SDNB network, but instead using a provider's data plan. However, please remember that the expectation is that devices will only be used for educational purposes during the school hours and teachers retain the right to require students to not use a device if they believe it is not being used for something educationally based.

<div>+</div> *I have my own laptop and a smart phone. I would like to utilize these tools at work. Does this new plan include campus staff?*

Answer: Yes. Staff can also access the guest network. Keep in mind that the guest network is going to be filtered at the <u>student level</u> for anyone who may choose to access it.

<div>+</div> *I believe one of my students may have been using his laptop to bully another student. Should I call the technology office concerning this problem?*

Answer: No. Any disciplinary infractions that occur from using technology tools should be referred to a school administrator. This would be a student code of conduct issue.

↯ *Will students have access to any common software packages via the guest network access?*

Answer: Not at this time, but we are looking into options for this for a future tech rollout.

↯ *Should I call the tech office if one of my student's laptops is damaged or stolen?*

Answer: No. Any theft issues should be handled as you normally would on your campus. SDNB is not responsible for any damage or theft of student owned technology tools. It would be good to remind students to keep a record of the device's serial number just in case a theft occurs.

PARENTS

↯ *My child is bringing his iPad to school for instructional purposes. Will they have access to things they normally do with district equipment?*

Answer: Your child will have access to any of the web based software high school campuses currently use (Databases, library search tools etc.). Software may run differently on different devices for varying reasons. You should consult your owner's manual for software limitations. (Ex. iPads cannot run software requiring Flash Player).

↯ *As a parent, am I required to add additional software (virus protection, filter, tracking device etc.) to my child's technology tool?*

Answer: No. Currently we are not requiring any additional software for school use. Virus protection is always advised, but not required. While on the SDNB guest network, students will be monitored through the district's filter so there is no need for additional filtering software.

↯ *I have read the terms of service and I do not wish to have my child accessing the Internet using their own laptop. I would like to allow them to continue using their computer for productivity, but not the Internet. Is this allowable?*

Answer: Yes, you may choose to decline the terms of use. However, the rules outlined in the AUP still apply for technology use of any kind (Internet or other).

↯ *I am the president of a booster club at my student's school. We hold meetings at night. Will we have access to the SDNB guest network after school hours for our meetings?*

Answer: Yes. The guest network will be accessible after school hours.

↯ *If my child's laptop is stolen or damaged, what recourse can I take?*

Answer: The district is not responsible for any damage or theft of student owned equipment. Installing tracking software on your own device may help locate the equipment if it is stolen, and keeping track of the device's serial number, model and type will be helpful as well. Theft or vandalism of any kind should be reported immediately to a school administrator so they can take appropriate steps.

🞡 *What are the campus/classroom rules for using student owned devices including phones?*

Answer: The intention of devices during the school day is that they will be used for educational purposes only. Teachers make the decisions for any tools used in the classroom; student owned equipment will be no different. It will be up to the individual teachers to communicate their expectations to parents and students for their specific classes and courses.

🞡 *Will my child have access to communication tools like email or message boards while on the SDNB guest network?*

Answer: All students have the same level of access to these tools as they do on school-issued devices. While some forms of email and some message boards will be blocked by our content filter, district provided email and digital resources will not be blocked while at school.

Student Technology Guide

Revised Fall, 2013

The School District of New Berlin Information Technology Vision Statement

To expand an information and technology environment that uses twenty-first century learning to develop students, staff, and community members who effectively innovate, create, evaluate, and communicate learning through a collaborative and reflective community that is associated with the leaders in technology integration in education.

School District of New Berlin Appropriate Use Policy

Philosophy

The School District of New Berlin uses technology resources, including the Internet, as a tool for research and education. The Board of Education supports the use of its technology resources and its Web resources, including the Internet, to access resources and reference materials to meet educational and information needs.

The terms "technology resources," "networks" or "computers" used in District Policy are generally synonymous and include laptop computers, desktop computers, cell phones, telephones, servers, storage media, handheld devices, pagers, printers, scanners, software and other District-owned or contracted-for electronic communication equipment. Technology resources, like any other school property, are owned by and the property of the District or subject to the District's rights under contract and law. Technology resources must be used in the interests of the District and for the educational purposes for which it was intended. Users are required to follow the guidelines outlined in this Policy, administrative guideline and other related policies, guidelines and rules.

Web resources are a collection of tools that enable interaction on the Internet. Web resources include the Internet, blogs, wikis, podcasts, social-bookmarking, social networking sites, multi-user role-playing environments, video games and other forms of electronic communication. The District permits responsible and safe use of these tools for instructional and educational purposes. Users are expected to engage in safe and acceptable use of the Web resources. The information available via the Internet is constantly changing. Since it is impossible to predict with certainty what information individuals might locate, making electronic information available to individuals does not imply endorsement of that content by the District.

The use of technology resources and Web resources are considered extensions of the classroom. Therefore, compliance with all District policies, guidelines, rules and acceptable standards of behavior are necessary and required. Any communication that is considered inappropriate in the classroom is also inappropriate in all uses of Web resources. This includes but is not limited to profanity or racist, sexist or discriminatory remarks. The District prohibits users of the District's network from using, accessing, storing or transmitting inappropriate content. Examples of inappropriate content include offensive, profane, abusive, harassing, sexually explicit, threatening or obscene language or visual depictions, as well as pornography and child pornography.

Limitations/Privileges/Privacy

Technology resources provided by the District are for educational purposes only. Appropriate uses are those which support the District's mission and vision. Use of technology resources is a privilege. A user will be held responsible for his or her actions and obligations. This privilege may be revoked by the District in its sole discretion. Users of the technology resources will annually review the current acceptable use policies and guidelines.

The District is not liable for any damage suffered by a user of the system, including but not limited to, loss of data stored on or transmitted by technology resources or interruptions of service. The District is not responsible for any mistakes or negligence, liability, copyright infringements or other costs incurred by the person using the District's technology resources, or the accuracy or quality of information received over the Web resources. Copyright infringement, which may include the duplication of software or works, is a violation of the law and Board policy.

Users should have no expectation of privacy in the contents of any communications or files on District technology resources or Web resources unless such expectation is granted by law. The District has access to its technology resources and District-sponsored Web resources and maintains the right to access, inspect, investigate and monitor all use and its resources, including all files, communications and information created on, with or transmitted using its technology resources or Web resources, and including e-mail, text messages, internet usage, and any other communications or information, without notice to or consent of the user. All such files, communications, or information can be reviewed by the District for any purpose and at any time, and may be subject to monitoring, review and disclosure pursuant to civil and criminal matters, investigatory purposes, or any other lawful reason.

School officials reserve the right to discipline users who violate terms of this Policy and procedure, which may result in suspension of technology privileges, legal action, and discipline up to and including suspension and expulsion for students and discipline up to and including discharge for employees.

Parental Opt-Out Provision

The District will provide students access to technology resources, including the Internet, unless the parent/guardian notifies the appropriate building principal in writing that the District should prevent access to technology resources for his/her student(s). Parents or guardians have the right to view contents of their child's user account or network activity, if possible, accessible and within the confines of applicable law, or to revoke their child's technology permissions, upon written request.

CIPA (Children's Internet Protection Act)

It is the Policy of the School District of New Berlin to: (a) prevent access to or transmission of inappropriate content in its computers and over its network through electronic mail or other forms of communication; (b) promote the safety and security of minors using the District's computers, electronic mail, chat rooms, text messaging, instant messaging and other forms of communications; (c) prevent unauthorized access (such as "hacking") and other unlawful activities; (d) prevent unauthorized online disclosure, use, or dissemination of student personally identifiable information; and (e) comply with CIPA— the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)] and all other applicable laws.

The District uses an Internet content filtering system to limit access to material that is harmful to students, obscene or disruptive to the educational or work environment, and to a lesser degree, high risk activities. The District uses software designed to filter and block access to pornographic Internet sites. The District uses commercially reasonable technology protection measures designed to comply with CIPA's requirements. The District reserves the right to block sites that do not enhance educational activities or are not in compliance with CIPA. No technology measure can block 100% of inappropriate content so the District emphasizes the importance of responsible use and of parent and staff supervision in monitoring use of technology.

Education, Supervision and Monitoring
It shall be the responsibility of all instructional members of the District and parents to educate, supervise and monitor appropriate use of the online computer network and access to the Internet in accordance with this Policy.
The District will promote safe online activity for students and educate students about appropriate online behavior, including interacting with other individuals on social networking websites and cyberbullying awareness and response. This includes, but is not limited to:

- Teaching students how to locate and evaluate appropriate electronic sources;
- Teaching students information literacy skills, including understanding of safety, copyright, ethical practice and data privacy; and,
- Teaching students proper safety procedures when using e-mail, social networking websites, texting, and other forms of direct electronic communication.

Home and personal Internet or other communication tool technology use can have an impact on the District, school and others. If Internet expression creates a substantial disruption at school, offenders may be subject to school disciplinary action and/or legal action. Substantial disruption includes, but is not limited to, any of the following:

- Necessary cessation of instruction or educational activities;
- Inability of students or educational staff to focus on learning or function as an educational unit because of a hostile environment (including cyberbullying);
- Severe or repetitive disciplinary measures are needed in the classroom or during educational activities;
- Exhibition of other behavior by students that substantially interfere with the learning environment;
- Threatening acts or behavior to personnel and students; or,
- Endangering the health and safety of others.

Internet expression that creates a substantial disruption at school is a violation of this Policy and may be a violation of other District policies, guidelines and rules.

Non-District-Provided Technology
The District permits approved use of personal technology devices by students and staff in support of teaching and learning, managing resources, and connecting with stakeholders. Personal devices must meet minimum requirements for network access. Limited use of personal devices is permitted so long as it does not interfere with educational or employment responsibilities and as long as the use does not hinder, disrupt or consume an unreasonable amount of network resources, violate state or federal law, or Board policies.
Users may bring personal devices into the District to access the District network. Personal devices may include laptop computers, portable digital assistants (PDAs), cell phones, iPods/MP3 players, wireless devices, digital cameras, storage devices, or other electronics that may be carried on a person. This typically will include using the technology during class time but only when given express permission to do so by the classroom teacher and only for educational purposes. The District is not liable for the loss, damage, or misuse of any personal device including while on District property or while attending school-sponsored activities. Users that make use of any personal technology must follow all rules and guidelines of this Policy and related policies, guidelines and rules.

Individual building principals may establish specific guidelines regarding the use, nonuse or scope of permissible use of personal devices at their individual schools. These guidelines shall not be less restrictive than the direction given by the Board in its policies.

Connected to Policy 5131.13, Locker Room Privacy, Locker rooms are provided for the use of physical education students, athletes and other activity groups and individuals authorized by the Administration. No cameras, video recorders, cell phones or other personal devices may be used in locker rooms or rest rooms. No devices may be used to record or transfer images or sound in the locker room or rest room at any time.

Consequences
Inappropriate use of the District's technology resources, Web resources or District property and any other violation of District policies, guidelines or rules may result in suspension of technology privileges, report to criminal authorities, legal action, and discipline up to and including suspension and expulsion for students and discipline up to and including discharge for employees. Specifically, users are notified that sexually explicit or pornographic content has no place in the District and violators who use or access such content will face severe consequences including expulsion or termination. In addition, violations may result in financial charges for repair, replacement or services, as well as legal action. Appeals may be made in accordance with appropriate Board policies, procedures, employee contracts and student handbooks. Administrators may confiscate and search personal devices while on District property if the administrator has reasonable suspicion that the use of the device or technology is in violation of this Policy. The District will cooperate fully with local, state or federal officials in any investigation related to any illegal activities conducted through the District's systems.
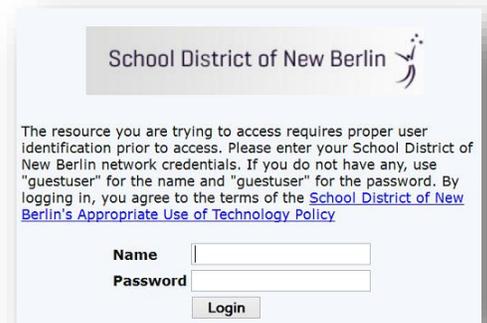
Accessing the Guest Network – New Splash Page

When you bring in your own device to use on the guest network, you will now need to log into the network through what is called a Captive Portal. This is something you would see at a hotel or conference center (accepting the terms of use - the Appropriate Use Policy - and logging in with network credentials). This will allow you to use your own device to gain the permissions they are assigned by your network administrator when connecting to the Internet (for filtering purposes). When using the Guest Network students and staff would use their regular network credentials as identification. This could provide increased browsing capabilities for Staff when using their own devices or District issued iPads.

Follow these directions to connect to the guest network: *You will need to complete this process every day you log into the SDNB GUEST wireless network. You will also need to complete this process any time your device experiences 45 minutes of inactivity.*

Setting up a wireless connection at school – Laptop or Windows/Android Tablet

- Log on to your device as you would outside of school.
- Click on the **SDNB GUEST** network from the Wireless Connections list and click on Connect.
- You will be connected to the Guest Network, but will not have any access.
- Launch your Internet browser. After the page loads, you will see the screen to the right.
- You will be asked to enter your **network User ID and network Password** and click Submit. You will need to enter this information on this page before you will be able to access the guest network.
- Once you access the wireless network, you can connect to the Internet using the browser on your device.

**Setting up a wireless connection at school – iOS device (iPad, iPod, iPhone)**

- In the device Settings, choose Network settings. When Wi-FI is on, choose **SDNB-Guest**. Once the network is selected, you will see the Wi-Fi signal in the upper left hand corner.
- You will be connected to the Guest Network, but will not have any access.
- Launch your Internet browser (Safari) and type in an Internet address in the address bar. After the page loads, you will see the screen to the right.
- You will be asked to enter your **network User ID and network Password** and click Submit. You will need to enter this information on this page before you will be able to access the guest network.
- Once you access the wireless network, you can connect to the Internet using the browser on your device. All of your apps should
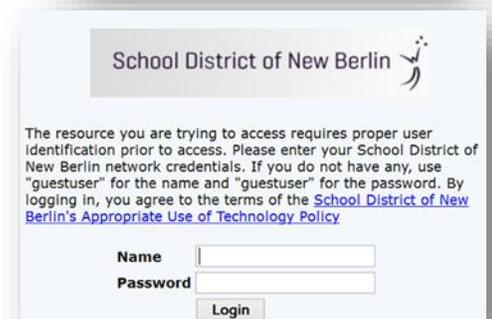
LL 9.2013

now also work based on your network permissions.

Student Expectations Regarding School Issued Technological Devices

As a learner I will…
1. Look after my device carefully all of the time.
   o Devices will never be left unattended
   o Devices must be situated securely on the working surface
   o Make sure the device is not subject to careless or malicious damage (i.e. as a result of horseplay)
   o Take care when the device is transported that it is as secure as possible. Laptops MUST be carried in its protective case at all transportation times outside of the classroom.
   o Carry the device in the closed position with two hands in the classroom.
2. Ensure that my device is plugged in and charging when not in use (i.e. plugging it in to the cart for charging overnight).
3. Be on the task assigned by my teacher at all times. Devices will ONLY be used for educational purposes as directed by New Berlin School District staff.
4. Return the device in the same condition that I checked it out in (if there are issues with the laptop that you are assigned, please report any issues immediately – this includes missing keys, graffiti, in appropriate access, etc.). **Students who return damaged devices may be subject to replacement costs.**
5. Use the pre-installed software or online resources. Please do not install additional software without express permission from the technology department.

General Maintenance of Laptops & File Management
When turning off
- Double check that you have saved all files and have quit all programs before shutting down
- Make sure that the computer is completely shut down before closing the lid. If you close it without it bing shut down, the computer will still use power and could damage the battery.

Battery Life / Charging
- Check battery levels and charge when battery is low. If your computer looses all battery power, you may lose any current open work. You may plug in your device as needed with permission from your classroom teacher.

File Management - Saving
In order to stay organized, it is important to save your documents in the correct folders. You can save your files to your network storage (H Drive) or a USB flashdrive. You can also upload and save files to your H: drive though Stoneware. Your teachers can give suggestions for folder structures to make saving and finding documents easy.

Digital Resources Reference Sheet

Stoneware - Stoneware is a web portal that allows students to access school network files and common links. This portal will be accessible at school and at home, providing students the unique opportunity to have access to network resources 24/7. The Stoneware portal will include links to the websites below.

- Access: http://cloud.nbexcellence.org/
- Stoneware Help documents – Please see Stoneware log-in screen.

E-mail – The district uses email to communicate with its student population. Many teachers also use email to communicate information about their class with students. You may also use the district email to contact your teachers or other students in your classes to help with your school work. As a reminder, all messages sent or received via the District e-mail system are the property of the District and may be reviewed, accessed, and disclosed as deemed necessary by the District. Transmitting spam messages, chain letters, or inappropriate e-mail may be considered a violation of District policies and procedures and may result in disciplinary action. (Policy reviewed 2/14/11)

- Access: http://login.microsoftonline.com

Infinite Campus - Infinite Campus is the student information system that the District uses to track student and household information. Infinite Campus is also used to post announcements, grades, and report cards.

- Access: http://www.nbexcellence.org/students/do_ic_students.cfm
- Infinite Campus Help documents - http://www.nbexcellence.org/students/do_ic_students.cfm

Moodle – Moodle is an interactive content management site, learning management system, or virtual learning environment. Your teachers may use Moodle to post assignments, share documents, provide links to homework, or accept homework that you complete.

- Access: http://moodle2.nbexcellence.org/
- Moodle Help documents - http://docs.moodle.org/en/Student_FAQ

REMINDERS:
- Student user IDs are typically the 1st and last initial and 4 random numbers (Example – John Smith – js3456).
- Passwords are case sensitive.
- School policy prohibits the sharing of any personal account information for the safety and security of your account and the school network.