TECHNOLOGY USE POLICY FOR EMPLOYEES

I. Staff Use of Computerized Information Resources

The Board of Education will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks and electronic communication systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may also include the opportunity for some staff to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use off school premises, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent or his/her designee(s) to provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon written agreement by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. All such agreements shall be kept on file.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff and to model appropriate and professional behavior. Electronic mail and telecommunications should not to be utilized by teachers to share confidential information about students or other employees with each other.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior.

District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further 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.

II. Social Media Use by Employees

The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance

student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Board of Education encourages the use of District approved social media tools and the exploration of new and emerging technologies to supplement the range of communication and educational services.

For purposes of this Policy, **public social media networks or Social Networking Sites (SNS)** are defined to include: Web sites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other social media generally available to the School District community which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, blog sites, etc.). The definition of **District approved password-protected social media tools** are those that fall within the District's electronic technology network or which the District has approved for educational use (e.g., Edmodo, Intranet). Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access.

The use of social media (whether public or internal) can generally be defined as Official District Use, Professional/Instructional Use and Personal Use. The School District takes no position on an employee's decision to participate in the use of social media or SNS for personal use on personal time. However, personal use of these media during District time or on District-owned equipment is limited in the manner set forth in District Regulation 4526.4-R. In addition, employees are encouraged to maintain the highest levels of professionalism. They have responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District Policies and Regulations.

Privacy Rights

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The Director of Technology or Superintendent may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should **NOT** expect that information stored on the DCS will be private.

III. Bring Your Own Device (BYOD)

This policy provides standards and rules of behavior for the use of personally owned smart phones, computers, tablets, and/or other electronic devices by Newfield Central School District employees (herein referred to as users) to access Newfield Central School District network resources. Access to and continued use of network services is granted on condition that each user reads, signs, respects, and follows the Newfield Central School District's policies concerning the use of these devices and services. It is expected that these personal electronic devices will only be used for school business reasons on school time and according to the Computer Use Agreement, except for emergencies or in extenuating circumstances.

Expectation of Privacy

Newfield Central School District will respect the privacy of personal devices and will only request access to the device to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings related to his/her employment. This differs from policy for district-provided equipment/services, where district employees do not have the right, nor should they have the expectation, of privacy while using district equipment or services. While access to the personal device itself is restricted, Newfield Central School District Policy and rules of behavior regarding the use/access of district e-mail and other district system/service remains in effect.

Overall Requirements for all BYODs Accessing Newfield CSD Network Services:

1) User will not download or transfer sensitive school business data to his/her personal devices. Sensitive school business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or agency financial operations;
2) User agrees not to use any unlicensed software;
3) User will be able to identify his/her device by serial number;
4) User will password protect the device;
5) User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls);
6) User agrees to delete any sensitive school business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. Newfield Central School District IT will provide instructions for identifying and removing these unintended file downloads if requested.
7) User understands that tech support will not be provided by the district except for installation and use of VDI software.
8) User assumes all responsibility for breakage, damage, theft, and data theft of his/her personal device.
9) User agrees not to allow student use of his/her personal device without prior administrative approval.
10) User is responsible for the content on his/her personal device and agrees to only share appropriate instructional content with students or other school employees.
11) User agrees the District is not liable for breakage, damage, theft, data theft, or failure in his/her personal device(s).
12) User acknowledges that the District will not reimburse for any expenses related to the use of a personal device pursuant to this policy, included but not limited to fees or access charges assessed by the user's wireless service provider.
13) Employees are permitted to connect their devices to District-owned devices only with the Director of Technology or Superintendent approval. Connection to projectors for classroom use may be done without prior approval.

TECHNOLOGY USE FOR EMPLOYEES REGULATION

Staff Use of Computerized Information Resources

The District's computer system (DCS hereafter) is provided for staff to enhance the educational programs of the District, to further District goals and objectives; and to conduct research and communicate with others.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. The standards of acceptable use as well as prohibited conduct by staff accessing the DCS, as outlined in District policy and regulation, are not intended to be all-inclusive. The staff member who commits an act of misconduct which is not specifically addressed in District policy and/or regulation may also be subject to disciplinary action, including loss of access to the DCS as well as the imposition of discipline under the law and/or the applicable collective bargaining agreement. Legal action may also be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

Staff are encouraged to utilize electronic communications in their roles as employees of the District. Staff are also encouraged to utilize electronic means to exchange communications with parents/guardians or homebound students, subject to appropriate consideration for student privacy. Such usage shall be limited to school related issues or activities. Electronic mail and telecommunications should not to be utilized by teachers to share confidential information about students or other employees with each other. Communications over the DCS are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The District's policies and accompanying regulations on staff and student use of computerized information resources establish guidelines for staff to follow in instruction and in working with students on acceptable student use of the DSC, including access to external computer networks.

Privacy Rights

Staff data files, District email and electronic storage areas shall remain District property, subject to District control and inspection. The Director of Technology or Superintendent may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of District policy and accompanying regulations. Staff should **NOT** expect that information stored on the DCS will be private.

Prohibitions

It is not the intention of this regulation to define all inappropriate usage. However, in addition to the general requirements of acceptable staff behavior, activities which shall be prohibited by staff members using the DCS include, but are not limited to, the following:

1) Using the DCS which in any way results in unauthorized charges or expense to the District.

2) Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.

3) Using unauthorized software on the DCS.

4) Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the staff member without express permission from the Director of Technology.

5) Violating copyright law, including the illegal file sharing of music, videos and software.

6) Employing the DCS for commercial purposes, product advertisement or political lobbying.

7) Disclosing an individual password to others or using others' passwords.

8) Sharing confidential information about students and/or employees.

9) Sending or displaying offensive messages or pictures.

10) Using obscene language.

11) Harassing, insulting, bullying, threatening or attacking others.

12) Engaging in practices that threaten the DCS (e.g., loading files that may introduce a virus).

13) Violating regulations prescribed by the network provider.

14) Use of the DCS for other than school related work or activities except for during breaks, lunch, or non-instructional time.

15) Assisting a student to violate District policy and/or regulation, or failing to report knowledge of any student violations of the District's policy and regulation on student use of computerized information resources.

16) Use which violates any other aspect of School District policy and/or regulations, as well as local, state or federal laws or regulations.

Any user of the DCS that accesses another network or other computer resources shall be subject to that network's acceptable use policy.

Sanctions

The Director of Technology will report inappropriate behavior to the staff member's supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the DCS and/or disciplinary action. When applicable, law enforcement agencies may be involved.

Notification

All staff will be given a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Each staff member will sign an Acceptable Use Agreement before establishing an account or continuing their use of the DCS.

Social Media Guidelines for Employees

Social media and social networking sites (SNS) have great potential to connect people around the globe and enhance communication; however, they are also more informal, less structured and constantly changing. These guidelines are designed to establish some basic parameters on the creation and use of SNS and other social media for the District and its personnel.

For purposes of this regulation, **public social media networks or Social Networking sites (SNS)** are defined to include: Web sites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other social media generally available to the public or consumers and which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, blog sites, etc.). The definition of **District approved password-protected social media tools** are those that fall within the District's electronic technology network or which the District has approved for educational use (e.g., Edmodo, Intranet). Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access within these internal forums.

Official District Use

Official District use is defined as the use of social media by an employee, on behalf of his or her department, program or school that has been authorized for the express purpose of communicating the District's broad interests or specific programmatic and policy interests. The authorization may be granted by the Superintendent or his/her designee. For example, the School District may decide to have its own official Facebook page. Or employees could be authorized to develop other pages dedicated to a single building, program, or sports team. There are also many official uses of social media that are not public, such as the use of internal blogs or wikis for collaboration among grade-level or project teams. Employees are prohibited from setting up public social networking sites for any official District use related to their division, building or service unless they have obtained prior approval in accordance with the procedures set forth below.

Establishing a Social Networking Site for Official District Use

1) Following approval from the Superintendent, technology staff will work with the department, building or service to properly set up an appropriate social networking site. All account names and log in passwords must be on file in the Technology Department.

2) The Superintendent/designee shall have the exclusive and final authority to determine whether individual buildings/facilities may initiate and maintain separate page(s) on the SNS.

Quality Control/Content Integrity

1) The District shall provide general training for all applicable personnel, including training on ethical and legal considerations, and compliance with all applicable policies and regulations.

2) The official District Web site will remain the primary source for all content. Any and all material on the District SNS will only supplement information that exists on the District's official Web site.

3) All the material/content that is entered or posted to the District SNS (e.g., Facebook) account/page must include a link back to the official District Web site or relevant partner. An occasional reminder or announcement without a link is permissible (for example, a "Save the Date" announcement).

4) Photos and/or identifiable student work should only be posted on the District-owned Web site that the SNS can link to. For control purposes, do NOT upload images of students directly on to a SNS.

5) Do not post confidential or proprietary information about the District, its students, alumni or employees. Use good judgment and follow District policies (i.e., FERPA).

6) Thoroughly spell check and grammar check your content before posting. Citizens expect that education employees will set a good example when they write and speak in public. Be professional.

7) Remember you are writing for publication, even on social networks. Refrain from making unsubstantiated statements. Always provide full citations for laws or research.

Disclaimers

The School District is an agency that is not liable for the content or comments posted to public social media sites. Any inappropriate content may be removed.

Professional or Classroom Use

Professional use is defined as an employee's use of social media for the purpose of furthering his or her specific job responsibilities or professional duties through an externally focused site or a district sponsored site. For example, many teachers across the country have signed up for discussion forums on EdWeek.org to engage with other teachers in a community of practice. While use for professional interests is beneficial to the work of the District because it enables employees to stay informed on important issues or to collaborate with their peers, the social media tool or site the employee is using is not maintained or monitored by the district itself. The employee is accessing sites and setting up accounts owned by private entities to consume and exchange information. Again, internally, professionals often collaborate through various technologies, but professional use of social media implies going outside of the internal network of the district. Employees' participation in external social media for professional use, using district technology, equipment and email addresses or during the school day requires prior approval and is subject to the procedures set forth below.

Classroom use is defined as use of SNS in a classroom for instructional purposes. An example of classroom use may be the creation of a forum for class discussion taking place in a password protected online environment. Students can interact with their peers and their teacher to discuss a current class topic, sharing what they have discovered on the internet and voicing their opinions. Teachers can upload homework, post school notices, moderate discussions and share materials. This online portal develops writing skills, encourages research skills and promotes intellectual discussion. Staff must also obtain prior approval for classroom use of these internal forums and monitor student use.

Establishing Access

1) If you are participating in a social network site and/or blog for District-related professional use, it must be done with the approval of your supervisor or principal.

2) Use of outside social networking sites (such as Facebook) for classroom or instructional purposes is prohibited. The District does not permit any communication or contact between staff and students on non-district based SNS (i.e., Facebook, Twitter, etc.). Teachers are encouraged to use existing District or RIC established web tools such as teacher web pages within the District Web site, Angel, Edmodo, etc. to communicate with students, to assign and collect student work, or to provide online feedback to students.

3) The District may establish an Alumni page within its District SNS. Teachers and staff may interact with former students within this forum on the district site. Staff interaction with recent graduates outside of the district controlled environment is discouraged. Use caution when "friending" former students. Realize that many former students have online connections with current students. Information shared between school staff and former students is likely to be seen by current students as well.

4) The District understands that 21st century learning is constantly changing and that many sites that are currently "blocked" by the District internet filter may have educational significance for teacher and student use. If you would like to request that an online site be accessible to use for teaching and learning, submit a request to the Building Principal for review. A description should be provided of the intended use of the site and what tools on the site match your needed criteria. A link to the privacy policy for such sites should also be included.

Quality Control/Content Integrity

1) When using social media for professional purposes, always clearly identify yourself and your position with the District. Use your actual professional name - never create an alias or post as anonymous. Misidentifying yourself or providing false information may result in disciplinary action. The District email address attached to your name implies that you are acting on behalf of the District.

2) While engaged in professional use of social media, do not post confidential or proprietary information about the District, its students, alumni or employees. Use good judgment and follow District policies.

3) Thoroughly spell check and grammar check your content before posting. Citizens expect that education employees set a good example when they write and speak in public.

4) Remember you are writing for publication, even on social networks. Refrain from making unsubstantiated statements. Always provide full citations for laws or research.

5) District personnel acknowledge and agree that when they create or post material on the District SNS they are in effect "content publishers" and as such are subject to a host of ethical and legal obligations including, but not limited to, compliance with the federal Digital Millennium Copyright Act.

Personal Use and Responsibility

Personal use is defined as use that is not related to an employee's job duties for the District or his or her professional interests. For example, outside of work hours, an employee might create or maintain a blog related to a hobby, or a personal Facebook page containing news about his or her family and friends. An employee checking his or her personal Facebook page, sending out a personal Tweet, or watching the latest viral YouTube video are examples of personal use of social media during the work day.

1) Personal use of social media is strictly limited during work hours to breaks and in private (non-student) areas.

2) District employees are personally responsible for all comments/information they publish online. Be mindful that what is published will be public for a long time. Be sure to protect privacy.

3) Online behavior should reflect the same standards of honesty, respect, and consideration that are used in face-to-face contact, and be in accordance with the highest professional standards. District employees are expected to behave honorably in online spaces. Online activities or communications which are improper, unethical, illegal, or which cause undue discomfort for students, employees, parents, or other members of the school community should be avoided. Be mindful that illegal activities will be prosecuted and the District will fully cooperate with law enforcement.

4) Posting comments and having online conversations on social media sites makes those comments public and available to anyone who has any online access. Please be aware that even with the strictest privacy settings what is said online should be within the bounds of professional discretion. Comments expressed via social media under the impression of a 'private conversation' could end up being shared in a larger, more public domain.

5) Comments related to the District or School District personnel should always meet the highest standards of professional discretion. When posting, employees should act on the assumption that all postings are in the public domain. Remember that posted information could be interpreted as an extension of your office or classroom. What is inappropriate in your office or classroom is also inappropriate online. If posting comments or viewpoints on topics related to the District using any online medium be sure you state that the information is

representative of your views and opinions and not necessarily the views and opinions of the District.

6) Before posting personal photographs or avatars that represent you, consider how the images reflect on your reputation and professionalism. Also, remember not to use copyrighted images.

7) Due to the evolving nature of social web sites, District personnel should not use personal SNS to create or maintain personal relationships with students. For purposes of these guidelines, "personal relationships with students" shall mean any behavior or conduct that is unrelated to course work or official school matters. Such behavior may erode the professional authority and traditional roles of teacher and student within the District and may violate District policies and/or regulations.

   Teachers should not "friend" any students enrolled in the district Pre-K through 12. It is too easy for genuinely-intentioned and innocent comments and situations to be misinterpreted, resulting in potentially damaging consequences for everyone involved. If your position within the District calls for communication with students or parents and is educationally justifiable, the use of the District network, email. teacher web pages within the District Web site, and school-provided/owned equipment are suggested for use when communicating on-line.

8) While mindful of employees' First Amendment free speech rights, District personnel who participate in social networking web sites, including the District SNS, shall not post any material which may result in the disruption of classroom or District activities. The District is entitled to make such a determination based on the facts surrounding the material as the District reasonably believes them to be.

   Employees are encouraged to seek permission from the subject before posting photographs and videos of fellow employees taken on school property or at school-sponsored events. Due to the sensitive nature and potentially damaging consequences, posting photographs or information about currently enrolled students in any capacity is prohibited. Realize that many former students have online connections with current students. Information shared between school staff and former students is likely to be seen by current students as well.

School Logos

Within your personal social mediums, do not use any District or school logo without written permission from District officials. For official pages, the District will provide you with a profile image to use.

Reporting Requirements

District personnel shall be required to report known or suspected violations of the District SNS Guidelines to their Building Principal or immediate supervisor.

Disciplinary Sanctions

District personnel who violate any provision of the SNS guidelines shall be subject to appropriate disciplinary measures up to and including termination of

Overall Requirements for all BYODs Accessing Newfield CSD Network Services:

1. User will not download or transfer sensitive school business data to his/her personal devices. Sensitive school business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or agency financial operations;
2. User agrees not to use any unlicensed software;
3. User will be able to identify his/her device by serial number;
4. User will password protect the device;
5. User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls);
6. User agrees to delete any sensitive school business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. Newfield Central School District IT will provide instructions for identifying and removing these unintended file downloads if requested.
7. User understands that tech support will not be provided by the district except for installation and use of VDI software.
8. User assumes all responsibility for breakage, damage, theft, and data theft of his/her personal device.
9. User agrees not to allow student use of his/her personal device without prior administrative approval.
10. User is responsible for the content on his/her personal device and agrees to only share appropriate instructional content with students or other school employees.
11. User agrees the District is not liable for breakage, damage, theft, data theft, or failure in his/her personal device(s).
12. User acknowledges that the District will not reimburse for any expenses related to the use of a personal device pursuant to this policy, included but not limited to fees or access charges assessed by the user's wireless service provider.
13. Employees are permitted to connect their devices to District-owned devices only with the Director of Technology or Superintendent approval. Connection to projectors for classroom use may be done without prior approval.

Use of VDI Software

Newfield will employ Virtual Desktop Infrastructure (VDI) to grant access to Newfield's internal network and resources. VDI technology is a secure, safe, and scalable technology that can be used internally and externally on personal and district owned computers and tablets. Mobile and remote employees can work anywhere and still have access to their programs files. All resources remain secure inside Newfield's data center.

If a user will be using the device to access school files, s/he should make an appointment with the Director of Technology to install the VDI software when turning in the signed User Agreement and Acknowledgement Agreement.

Misuse

The District prohibits any misuse of a personal device on school property and at school events held elsewhere. Misuse may include, but not be limited to, accessing inappropriate content, taking photos or recording videos of students or faculty members without their prior consent, etc. Any misuse will result in disciplinary action and revocation of BYOD privileges.

BOE Adoption: May 7, 2013