

ELECTRONIC ACCESS REGULATION AND INTERNET SAFETY POLICY

The following rules and regulations govern the use of ~~district~~District technology. This includes computers, software, network resources, and access to the ~~Internet~~internet, as well as any third-party cloud services which are maintained by, contracted for, or otherwise used at the direction of the ~~district~~District, e.g., Office 365. (collectively “the network”)

These rules and regulations apply whether access to Islip network resources takes place from within the ~~d~~District or outside the ~~d~~District, and whether the resources being accessed are hosted within the ~~d~~District or elsewhere. See section XIII for additional information pertaining to remote access.

I. Administration

- The Superintendent of Schools ~~shall~~will designate the Network & Systems Coordinator to oversee the network.
- The Network & Systems Coordinator ~~shall~~will:
 - Monitor and examine all network activities, as appropriate, to enforce proper use of the network.
 - Ensure that all files and software are scanned for computer viruses.
 - Review the compatibility and technical requirements of, and approve all software whether onsite or web-based prior to purchase.
- The Assistant Superintendent for Curriculum and Instruction or designee ~~shall~~will:
 - Disseminate these rules and regulations at the building level with all network users.
 - Provide employee training for proper use of the network and ensure that staff provides similar instruction to their students, which ~~shall~~will include disseminating copies of these rules and regulations. Said training ~~shall~~will include the education of minors regarding appropriate online behavior, including interacting with individuals on social networking sites and in chat rooms, and cyber-bullying awareness and response.
 - Students and staff will receive training which will include an overview of potential consequences for violations of District policies related to electronic access and internet safety.
- All parental consent forms and student network-use agreements ~~shall~~will be kept on file in the principal’s office of the respective school or electronically within the ~~d~~District’s student information system.
- Staff members are responsible for teaching proper techniques and standards for participation, guiding access to appropriate sections of the network, and assuring that users understand that if they misuse the network, they may lose their access privilege. Particular concerns include network security, privacy, especially as it pertains to social networking sites, copyright infringement, E-

Mail etiquette, computer viruses and spyware, and proper use of the ~~World Wide Web~~internet and other network resources.

- All users will be provided with individual user accounts. The person in whose name the account is issued is responsible at all times for its proper use and security. Care must be taken to choose passwords which cannot be easily guessed. Passwords are not to be shared with anyone and must ~~be changed regularly and in accordance~~comply with requirements enforced by the network.

II. Network Access

The following people are entitled to use the network for authorized purposes provided they have agreed in writing to (and/or had a parent or guardian agree in writing to) these policies:

- All employees of the ~~district~~District for school business;
 - All ~~district~~District students, when under direct adult supervision, with signed parental permission slips;
 - Others working in K-12 public education who request use of the network. These requests will be reviewed on a case-by-case basis and will be granted as needs and resources permit by the Superintendent of Schools or his/her designee.
- Outside vendors, trainers, or contractors brought in at the ~~district's~~District's request, and solely for ~~district~~District-related business.

In order to provide appropriate security for the network, users may be required to enroll in two-factor authentication (2FA); this entails using both a password and an additional form of identification such as a one-time code to verify identity.

In the event a user elects to use a personal device (such as a cell phone) to receive one-time codes for 2FA, the device remains the property of and under the control of the user at all times. The ~~district~~District accepts no responsibility for the functionality of the device nor any costs that may be incurred by the user; additionally, no support can be provided for the device, nor does the use of the device imply any obligation on the ~~district's~~District's part to provide network access to it. Using a personal device to receive 2FA codes does not grant the ~~d~~District any access to the device or any content on it whatsoever.

If a user does not want to use a personal device for 2FA, other verification methods are available.

III. Acceptable Use and Conduct

Acceptable uses of the network are activities that support learning and teaching; inappropriate matter on the ~~Internet~~internet and the ~~World Wide Web~~ is prohibited. Network users are encouraged to develop uses which meet their educational needs

and which take advantage of the network's functions such as E-Mail, access to the ~~World Wide Web~~internet, and other ~~Internet online~~ resources.

Limited personal use of the ~~D~~istrict's computer system is permitted as long as it does not interfere with the discharge of an individual's job responsibilities and has no discernible cost to the ~~district~~District. Such use ~~shall will~~ be personal and not commercial in nature, and ~~shall will~~ not fall under any of the prohibited uses.

Islip Public Schools has taken measures to restrict both adults and minors from accessing materials that may be considered obscene, pornographic, or in the case of minors, harmful to them. The ~~e~~District utilizes a content filtering system which is updated regularly and automatically blocks access ~~to~~ undesirable web sites in compliance with the Children's Internet Protection Act (CIPA). Content may be explicitly blocked or permitted with or without notice at the discretion of the Network & Systems Coordinator as necessary. All web traffic is logged and may be monitored both in real-time and historically to detect inappropriate uses.

IV. Unacceptable Activity and Uses

Unacceptable uses of the network include, but are not limited to:

- Using profanity, obscenity, or other language which may be offensive to another user;
- Using defamatory, discriminating, or threatening language;
- Cyber-bullying;
- Using the network for financial or commercial gain;
- Sharing content that constitutes advertising either directly or indirectly for a third party unrelated to ~~school~~School ~~district~~District operations;
- Re-posting personal communications without the author's prior consent;
- Attempting to deliberately degrade or disrupt the computer system, which will be viewed as criminal activity under applicable state and federal law;
- Downloading, storing or printing files or messages that are pornographic, profane, obscene, or that use language that offends or tends to degrade others;
- Spreading computer viruses or spyware deliberately;
- Using the network for any illegal activity, including violation of copyright or other contracts;
- Vandalizing the data of another user or ~~district~~District equipment or materials;
- Creating, running, or installing programs that waste system resources, including but not limited to spyware, adware, and outdated or incompatible applications;
- Gaining unauthorized access to resources or entities;
- Invading the privacy of individuals (such as harassing, embarrassing, humiliating);
- Using an account owned by another user;
- Posting anonymous messages;

- Posting personal information when not related to a school purpose or activity, such as address, telephone number or school address;
- Unauthorized access, including so-called “hacking,” and other unlawful activities; which will be viewed as criminal activity under applicable state and federal law;
- Using network features such as chat rooms, peer-to-peer file transfer utilities, and instant message (IM) services, unless expressly permitted by the Network & Systems Coordinator;
- Unauthorized disclosure, use and dissemination of personal identification information regarding minors;
- Installing personal software on the ~~district’s~~ District’s computers under any circumstances; ~~Only~~ software licensed for use by the ~~district~~ District may be installed on ~~district~~ District computers, and must only be installed by the IT department following a properly approved software installation request;
- In limited circumstances, staff may be given permission to use a personal iCloud / iTunes account on a ~~d~~District-owned Apple IOS device; in this case, software purchased by the user may be used on the ~~d~~District’s device so long as doing so does not violate the software license to which the user agreed when purchasing the application. It is understood that licenses purchased by the user on a personal account remain the property of the user, however, care should be taken to not create excessive workflow dependency on applications that are not owned by the ~~d~~District. The ~~d~~District reserves the right to remove this permission at any time and for any reason.
- Using personal devices or peripherals on the ~~district’s~~ District’s computers and/or network without the permission of the IT department;
- Saving data in any location other than those designated by the IT department;
- Attempting to bypass the ~~district’s~~ District’s security measures or content filtering in any manner;
- Using the network while access privileges are suspended or revoked; and
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

Network users identifying a security problem on the ~~district’s~~ District’s network must immediately notify the appropriate teacher, administrator and/or the Network & Systems Coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the ~~district~~ District official or employee being notified.

V. *Social Networking*

The growth of social networking sites ~~such as Facebook~~ creates a unique challenge in the school environment. These types of sites often bridge a user’s personal and professional life and thus put the user at significant risk of disclosing information or inadvertently acting in a fashion that is inappropriate in a school setting.

All staff are to be mindful of professionalism when posting on social media sites, as postings could impact your professional reputation and the reputation of the School District.

Personal student information is not to be shared on social networking sites under any circumstances.

~~Outside the sphere of school business, the district~~ District recommends prohibits staff ~~not from~~ “friending” or “following” any current student ~~regardless of age~~, or any former student under the age of 18 ~~other than a relative~~.

VI. *Use of Personal Devices (Bring Your Own Device – “BYOD”)*

Under certain circumstances, certain users may be afforded the opportunity to connect their personal devices to a ~~portion of the wireless~~ network designated for this purpose. If a user elects to do so, such use is subject to the following:

- All regulations detailed elsewhere in this policy remain in full force on any BYOD network;
- No support will be provided for personal devices; there is no guarantee a given device will function on the network;
- The ability to connect may be restricted (either by policy or by technical limitations) to those devices which are kept up to date with supported operating systems, security patches and antivirus; in this event any efforts to remediate these issues are the sole responsibility of the device owner;
- Users may be required to validate their identity to the network at a regular interval to verify their permission to use the system;
- Any BYOD network made available should be assumed to be insecure, and users should take appropriate measures to protect their devices from other devices sharing the network;
- In the event any BYOD network creates a security or performance issue with the ~~district’s~~ District’s “production” network, or as necessary for network maintenance or upgrades, it may be temporarily disabled without notice;
- The availability of any BYOD network is provided at the discretion of the ~~district~~ District and may be terminated at any time;
- The user’s rights to access a BYOD network may be terminated at any time for any violation of ~~D~~istrict policy or if their device(s) create a disruption in service to other users or to the network as a whole;
- The use of a BYOD network does not eliminate the ~~district’s~~ District’s legal obligation to comply with CIPA (see Section XII), and as such all internet access on a BYOD network remains filtered; users may be required to validate their identity to the content filtering system in order to receive the appropriate filtering policy;
- Any other restrictions necessary to ensure the safety, security, and reliability of the ~~district’s~~ District’s network, as determined by the Network & Systems

Coordinator; these may be changed at any time, for any reason, and without notice.

VII. *Electronic Publications*

Users will be allowed to produce materials for electronic publication on the ~~Internet~~[internet](#). -Staff supervisor of user will monitor these materials to ensure compliance with content standards. -The content of materials is constrained by the following restrictions:

- Student information and/or work used for electronic publication on the ~~Internet~~[internet](#) will correspond to the level of parental consent on the student's Parental Consent Form.
- No text, image, movie or sound that contains pornography, profanity, obscenity or language that offends or tends to degrade others will be allowed.

VIII. *No Privacy Guarantee*

It should be understood that use of the ~~district's~~[District's](#) network is not private and that network use, including the content of E-Mail sent or received, may be monitored at any time and without notice. The ~~district~~[District](#) reserves and may exercise the right to monitor, access, retrieve, or delete any data stored in, created, received, or sent over the ~~district's~~[District's](#) network and/or E-Mail system from any device, for any reason, without permission, and with or without cause.

If an authorized user of the ~~district's~~[District's](#) E-Mail system would like to access e-mail from outside the ~~district~~[District](#), there are two methods that may be used:

- Visit [Office365 \(https://portal.office.com\)](https://portal.office.com) from any compatible web browser and select the Outlook tile, *or*
- From your smartphone or tablet, via ActivSync or similar "push" technologies; this includes the native mail application on most devices as well as the Outlook "app"

Regardless of how a personal device is connected to or otherwise used to access the ~~district's~~[District's](#) email system (or other ~~district~~[District](#)-owned systems such as Infinite Campus), the ~~district~~[District](#) **does not have the ability** to access any photos, contacts, text messages, or other personal data on said device, and will not use any such abilities to do so should they become available in the future. All personal data remains the property of the device's owner and the ~~district~~[District](#) will respect the privacy of this personal data.

When an authorized user elects to use ~~ActivSync (or similar "push" technologies)~~ ~~to connect a mobile e-mail app~~ to ~~connect to~~ the ~~district's~~[District's](#) e-mail system, the device establishes and maintains an always-on connection to the ~~district's~~[District's](#)

[District's](#) e-mail system, and as such may become subject to ~~district~~[District](#) policies concerning mobile devices.

It is important to note that when a device is connected to ~~our the District's~~ e-mail system *in this specific fashion*, the device may download and store data which may be confidential and which the ~~district~~[District](#) has a legal obligation to protect. In the event a personal device connected in this fashion is lost, cannot be retrieved, and cannot be locked, wiped, or otherwise secured by the device's owner, the ~~district~~[District](#) retains the right to remotely wipe the device if there is reason to believe the device may contain information which the ~~district~~[District](#) has a legal obligation to protect.

The ~~district~~[District](#) will not remotely wipe a device without first notifying the device's owner and providing a reasonable opportunity for the owner to retrieve or otherwise secure the device.

If it is determined a remote device wipe is necessary, the ~~district's~~[District's](#) e-mail system will be used to issue a command to wipe only ~~district~~[District](#) data from the device. Different devices and software versions may, however, respond to this wipe command differently, and thus the ~~district~~[District](#) cannot guarantee that additional data will not be removed. It is possible the user may lose personal content such as contacts and photos; under no circumstances will the ~~district~~[District](#) be liable for any such loss. It is always advisable to backup personal devices, regardless of the use of the ~~district's~~[District's](#) e-mail system.

Users who may be uncomfortable with the above provisions pertaining to personal devices may still access ~~district~~[District](#) e-mail from personal devices by logging on to Office365 via a web browser and selecting the Outlook tile. Connecting to this e-mail system via the web does *not* create an always-on ~~connection,~~ ~~and connection and~~ does *not* subject the device to the provisions outlined above.

Access permissions may be revoked at any time and with or without cause at the discretion of the Network and Systems Coordinator. Additionally, no support will be provided for devices which are not owned by the ~~district~~[District](#).

IX. Sanctions

All users of the ~~district's~~[District's](#) computer network and equipment are required to comply with the ~~district's~~[District's](#) policy and regulations governing the use thereof.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state, and/or local law or regulation is prohibited. This includes, but is not limited to material protected by copyright, threatening or obscene material, or material protected by trade secret.

Users must respect all intellectual and property rights and laws.

X. Damages

Care should be taken when using School District computers and other electronic devices. Parent(s)/Guardian(s) could be financially responsible for any damage to the computer/device.

XI. District Limitation of Liability

The ~~district~~District makes no warranties of any kind, whether expressed or implied, for the service it is providing hereunder. The ~~d~~District will not be responsible for any damages that a person may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruption caused by the ~~district's~~District's negligence or the individual's errors or omissions. Use of any information obtained via the ~~Internet~~internet is at the individual's risk. The Islip School District does not assume responsibility for the accuracy or quality of information obtained through its services.

In no event ~~shall~~will the ~~district~~District be liable for any indirect, special, or consequential damages or loss of profits arising out of or related to this agreement, the performance or breach thereof, or the accuracy or correctness of data or the information contained herein, even if the ~~district~~District has been advised of the possibility thereof.

In no event ~~shall~~will the ~~district~~District be liable for any damages resulting from or related to any failure or delay of the ~~district~~District in providing access under this Agreement or to the accuracy or correctness of the data or the information contained herein.

XII. Children's Internet Protection Act (CIPA)

In December 2000, Congress passed the Children's Internet Protection Act. -This act outlines requirements for any K-12 public school that receives funding under the E-Rate program for telecommunication services, ~~Internet~~internet access, and/or any direct costs associated with ~~Internet~~internet access.

Under this legislation, schools (including the school board) and libraries must:

- Create an ~~Internet~~internet safety policy and distribute it to their school community;
- Make this policy available to the FCC for review on request;
- Provide reasonable public notice and hold at least one public hearing or meeting to address the proposed or revised ~~Internet~~internet safety policy;
- Retain ~~Internet~~internet safety policies for a period of five years after the funding year the policy was relied upon to obtain the E-Rate funding

- Implement technology protection measures to prevent adults and minors from accessing inappropriate material, including visual depictions that are obscene, pornographic, or, with respect to the use of the computers by minors, harmful to minors.

XIII. Remote Access to District Resources

The modern computing environment includes both resources hosted within the eDistrict and others hosted by 3rd third parties in the “cloud.” Additionally, remote work, including work-from-home, has blurred the line between on-site and off-site work. For these reasons, the eDistrict makes no distinction between those activities originating from within the eDistrict and those originating from outside the eDistrict as they pertain to the policies herein. Users are expected to comply with all eDistrict network use policies regardless of their location, and regardless of the remote access technology used.

Third parties not employed by the eDistrict are required to sign the “INDIVIDUAL CONFIDENTIALITY AND REMOTE ACCESS AGREEMENT” in addition to the “EMPLOYEE AGREEMENT FOR ELECTRONIC ACCESS REGULATION” below.

[Adoption Date: October 18, 2005](#)

[Amended: November 21, 2006](#)

[Amended: March 20, 2007](#)

[Amended: July 7, 2010](#)

[Amended: August 30, 2012](#)

[Amended: February 20, 2013](#)

[Amended: April 3, 2013](#)

[Amended: February 25, 2014](#)

[Amended: October 20, 2014](#)

[Amended: August 25, 2015](#)

[Amended: January 19, 2016](#)

[Amended:](#)

NOTE: THIS PORTION OF THE POLICY WILL BE MOVED TO A SEPARATE POLICY (4526-R2) TO BETTER ALIGN THE ONLINE POLICY MANUAL

ELECTRONIC ACCESS REGULATION AND INTERNET SAFETY POLICY
FOR ISLIP EMPLOYEES

– E-MAIL, INSTANT MESSAGING, AND RELATED TECHNOLOGIES
(Collectively the “messaging system”)

The effective management and application of information technology improves the quality of service delivered to the Islip community, the productivity of ~~district~~District employees, and the overall cost effectiveness of ~~district~~District operations. Electronic mail (E-Mail) and Instant Messaging play an increasingly important role in meeting this challenge.

The ~~district~~District provides E-Mail ~~through Microsoft Office 365 and~~ and Instant Messaging (IM) through ~~both~~ Microsoft ~~Exchange and Office 365~~ Teams and Google Chat. No other e-mail ~~or IM or IM~~ systems ~~are to~~ be used for ~~district~~District purposes. These systems are integrated with each other; any reference below to one should be understood as applying to all as appropriate. In addition, any references to “the network” should be understood to apply as described previously in [policy](#) 4526-R.

GENERAL POLICY AND GUIDELINES

This policy outlines office requirements for the use and security of the Islip School District messaging systems, including the disclosure and monitoring of the contents of messages and electronic files stored in its system.

The Islip School District messaging systems are to be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of the Islip School District. Users must acknowledge their understanding of the general policy and guidelines as a condition for using the electronic mail system. Failure to adhere to this policy and its guidelines may result in suspending or revoking the offender’s privilege of using any part of, or the entire messaging system, and/or other sanctions.

- All electronic and telephonic communication systems, and all communications and information transmitted by, received from, or stored in these systems are the property of Islip School District. Limited personal use of the ~~district’s~~District’s e-mail system is permitted as long as it does not interfere with the discharge of an individual’s job responsibilities and has no discernible cost to the ~~district~~District. Such use ~~shall~~will be personal and not commercial in nature, and ~~shall~~will not fall under any of the prohibited uses.
- Employees may be permitted to use personal devices to connect to the ~~d~~District’s e-mail system ~~via ActivSync (or similar “push” technology)~~ at the discretion of the Network & Systems Coordinator. If permission is granted, it may be removed at any time with or without notice, and with or without cause. The ~~district~~District will not provide support for personal devices.

- Personal devices connected to the ~~district's~~ District's e-mail system via a mobile e-mail app ActivSyne (or similar "push" technology) may become subject to certain mobile device policies and restrictions as outlined in Section VIII of this regulation. In all circumstances, personal data remains the private property of the device's owner and no attempt will be made to access this data.
- The messaging systems may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, other non-job related solicitations, or in any other way that violates the ~~district's~~ District's no solicitation policy.
- Employees may not create automatic forwarding rules sending ~~D~~istrict e-mail to any outside address without approval from the Network & Systems Coordinator or their designee. Doing so may create a violation of FERPA, NYS Ed. Law 2D, or other applicable statutes.
- Employees have no right of personal privacy in any matter stored in, created, received, or sent over the ~~district's~~ District's messaging systems. The confidentiality of material cannot be assured under any circumstances.
- Use of passwords or other security measures does not in any way diminish the ~~district's~~ District's rights to access materials on these systems. The ~~district~~ District reserves and may exercise the right to monitor, access, retrieve, or delete any data stored in, created, received, or sent over the ~~district's~~ District's network and/or messaging systems from any device, for any reason, without permission, and with or without cause.
- Deletion of messages or files does not truly eliminate the messages from the system. E-mail and instant messages are archived and backed-up; consequently they may remain in our records forever.
- Employees are not authorized to retrieve or read any messages that are not directed to them without prior approval of the Superintendent of Schools or his/her designee.
- Employees shall-will not use ~~district~~ District provided messaging systems to create, send, or receive messages containing discriminating, intimidating, hostile, or offensive material concerning sex, race, color, national origin, religion, sexual orientation, age, marital status, disability, or any other classification protected by law.
- Employees shall-will be courteous and conduct themselves in a professional manner at all times.
- Care should be exercised to ensure all messages are sent only to the intended recipient(s), keeping in mind messages may be forwarded and thus read by people other than the original recipients.
- The ~~district~~ District messaging systems shall-will not be used to upload, download, or transfer copyrighted materials, trade secrets, proprietary financial information, or similar materials.
- Employees shall-will report to their immediate supervisor any message that threatens to endanger the safety of students, employees, or other persons.
- Any employee who discovers misuse of the messaging system should immediately contact the Network & Systems Coordinator.
- Users must be wary of ongoing security threats such as phishing e-mails, which are designed to solicit user's network credentials to then be used for malicious purposes. Care must be taken never to submit credentials to questionable sites; if

there is any doubt as to whether a request for credentials is legitimate, the employee should contact the Network Operations staff for clarification

[Adoption Date: October 18, 2005](#)

[Amended: November 21, 2006](#)

[Amended: March 20, 2007](#)

[Amended: July 7, 2010](#)

[Amended: August 30, 2012](#)

[Revised: February 20, 2013](#)

[Revised: April 3, 2013](#)

[Revised: February 25, 2014](#)

[Revised: October 20, 2014](#)

[Revised: August 25, 2015](#)

[Revised: January 19, 2016](#)

[Revised:](#)

NOTE: THIS PORTION OF THE POLICY WILL BE MOVED TO A SEPARATE POLICY (4526-E.2) TO BETTER ALIGN WITH THE ONLINE POLICY MANUAL

EMPLOYEE AGREEMENT FOR ELECTRONIC ACCESS REGULATION
(INCLUDING MESSAGING) AND INTERNET SAFETY POLICY

Employee Name _____ Building _____

I have read and understand the Electronic Access Regulations (including Messaging) and Internet Safety Policy statement. I accept the responsibility for abiding by those provisions. I understand that violation of the provisions stated in the policy may constitute revocation of network access.

“I will strive to act in all situations with honesty, integrity and respect for the rights of others and to help others to behave in a similar fashion. I agree to follow the access, usage, and content rules as put forth in the Islip School District’s Electronic Access Regulations and Internet Safety Policy, and I understand the potential consequences for not abiding to the same.”

Signature _____ Date _____

~~I hereby request the district enable mobile device access for my e-mail account so I may connect my phone or other mobile device to the district’s e-mail system and receive “push” notifications. In doing so~~In the event I elect to connect any personal devices to the district’s e-mail system, I consent to the terms and conditions established in Section VIII ~~above of policy 4526-R.~~ This consent will continue indefinitely unless I notify the ~~district~~ District otherwise in writing.

Signature _____ Date _____

Adoption Date: October 18, 2005
Amended: November 21, 2006
Amended: March 20, 2007
Amended: July 7, 2010
Amended: August 30, 2012
Revised: February 20, 2013

Revised: April 3, 2013

Revised: February 25, 2014

Revised: October 20, 2014

Revised: August 25, 2015

Revised: January 19, 2016

Revised:

NOTE: THIS PORTION OF THE POLICY WILL BE MOVED TO A SEPARATE
NEW POLICY (4526-E.3) TO BETTER ALIGN WITH THE ONLINE POLICY
MANUAL

INDIVIDUAL CONFIDENTIALITY AND REMOTE ACCESS AGREEMENT

Company or Organization: _____

Individual to be given access: _____

Primary contact at Islip Schools: _____

I am employed by (or work under contract with) the organization listed above, and in order to perform my work for the organization I will require access to the computer system of Islip Public Schools. As a condition of being allowed such access, I agree that:

- I will use only the log-in ID assigned to me by the Islip Public Schools when logging on to the Islip Public Schools computer system;
- I will log-off the Islip Public Schools system immediately upon completion of each session of service;
- I will not allow other individuals to access the Islip Public Schools computer system;
- I will keep strictly confidential the log-in ID and all other information that enables such access;
- I will not intentionally access any information or data other than that which I have been specifically authorized to access by the Islip Public Schools;
- I will not simultaneously access the internet or any other third party network while logged on to the Islip Public Schools computer system, unless strictly necessary for the execution of my contracted tasks;
- My access to the Islip Public Schools computer system is subject to monitoring by Islip Public Schools;
- I will not make any change to any of the Islip Public Schools systems without the prior written approval for the specific change from the Network & Systems Coordinator or his or her designee;

I also agree to keep strictly confidential all information to which I have access or which I otherwise acquire. I agree that I will not, directly or indirectly, disclose any Islip Public Schools information to any person except specified personnel of the School District and others providing services relating to the District who have a need to know to fulfill their job responsibilities and business obligations and have undertaken a similar confidentiality obligation.

I agree that I will not appropriate any information to my own use or to the use of any other person or entity. I further agree not to remove any information from District premises or systems without express permission from the individual named above as "Primary contact at Islip Schools", or that person's delegate.

By signing below, I agree to be personally bound by this agreement.

Signature

Date

Adoption Date: ~~October 18, 2005~~

~~Amended: November 21, 2006~~

~~Amended: March 20, 2007~~

~~Amended: July 7, 2010~~

~~Amended: August 30, 2012~~

~~Revised: February 20, 2013~~

~~Revised: April 3, 2013~~

~~Revised: February 25, 2014~~

~~Revised: October 20, 2014~~

~~Revised: August 25, 2015~~

~~Revised: January 19, 2016~~

