BABYLON UNION FREE SCHOOL DISTRICT
VIA ZOOM

BABYLON SCHOOL BOARD REGULAR BUSINESS MEETING
AGENDA
JUNE 22, 2020

I. Call to Order - 6:30 p.m.

II. Executive Session
It is anticipated that upon a majority vote of the total membership of the Board, a motion to meet in Executive Session to discuss specific collective bargaining, personnel issues, and/or other specific matters appropriate for executive session in accordance with the Open Meeting Law will be considered. Following executive session the Board will reconvene in the Babylon Junior-Senior High School library at approximately 7:30 p.m.

III. Pledge of Allegiance - 7:30 p.m.

IV. Approval of the Minutes of the Special Meetings of May 7, 2020, May 9, 2020, May 18, 2020.

V. Approval of Treasurer's and Business Office Financial Reports and Extra Curricular Fund Report for May 2020.

VI. Superintendent's Report
a. News & Updates Around the District

VII. Committee Reports
a. Audit Committee
b. Finance Committee
c. Buildings & Grounds
d. Technology Committee
e. Curriculum Committee
f. Policy Committee

VIII. New Business

1. **PART-TIME SECURITY GUARD APPOINTMENTS: RESOLVED**, that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following part-time security guard appointments effective July 1, 2020 to August 31, 2020 on an as needed basis during that period of time. Compensation for these positions to be at the security guard hourly rate of pay of $18.00, senior guard hourly rate of pay $22.00/hour*

James Wood	Gerard Grant	Michael Koubek	Michael Tenety*
Tina Cardinal	Tom Parsons	Kenny Meyerback	Joe Cautela
Justin Muller	David Cronemeyer	Dan McHugh	Mike Connelly
Maria McSweeney	John McSweeney	Ryan Bellittieri	Vinny Weiss
Thomas McGrane	Billy Walsh	Melissa Farrell	Michael Mertz
Michael Cusumano	Tony Buonincontri	Bobby Cralock	Timothy Bivona
Thomas Coll	Dan Gargan	Jeff Rhodes	Melaine Balsdon
Adolfo Berrios	Pat Walker	Alyssa Colletti	Mike Petriello
Joe Arlotta	Christina Dahling	Giacomo Sciuto	Scott Leinster

2. **PART-TIME DISTRICT COURIER APPOINTMENT: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves Lonell Rogers as a part-time District Courier from July 1, 2020 to June 30, 2021. Compensation for this position to be $18.00/hour.

3. **PART-TIME CUSTODIAL APPOINTMENTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following part-time custodial appointments from July 1, 2020 to August 31, 2020. Compensation for these positions to be at the part-time custodial rate of pay of $14.00/hour.
Jorge Cruz Bruno Estevez Miguel Estevez Charles Jacob Vincent Petrina Brian Ryan

4. **PART-TIME SCHOOL LUNCH MANAGER APPOINTMENT: RESOLVED**, that upon the recommendation of the Superintendent of Schools, the Board of Education approves the appointment of Nancy Padrone as a part-time school lunch manager effective July 1, 2020 to June 30, 2021. Compensation for this assignment to be $400.00/day, not to exceed 2.5 days per week.

5. **SUBSTITUTE CUSTODIAL APPOINTMENTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following substitute custodial appointments effective July 1, 2020 to August 31, 2020. Compensation for these positions to be at the substitute custodial rate of pay of $13.00/hour.

Jusine Alaggio	Milagros Anderson	Mercedes Bautista	Alexandro Berroa	George JaVurek
Alicia Metzger	Madeline Rivas	Leslie Witthohn	Wesley Ramkhalawan	

6. **CASUAL APPOINTMENTS: RESOLVED,** that the Board of Education approves the following coaching casual appointments for the 2020-2021 school year. Compensation for these positions to be in accordance with the Babylon Teachers' Association Contract for the 2020-2021 school year.

Varsity Cheerleading	Kara Bochicchio	($5720)
Varsity Boys Cross Country	Luke Merz	($5720)
Varsity Girls Cross Country	Adam Geller	($5720)
JH Cross Country	Eric Solnick	($4719)
Varsity Field Hockey	Emilee Rahner	($5720)
JV Field Hockey	Allison Buser	($4900)
JH Field Hockey	Olivia Cabral	($4719)
JH Field Hockey	Stephanie Greaney	($4719)
Varsity Football	Rick Punzone	($8158)
Assistant Varsity Football	Bill Singleton	($7319)
Assistant Varsity Football	Vinny DeLapi	($7319)
Assistant Varsity Football	Steve Fasciani	($7319)
Assistant Varsity Football	Tim Halvorsen	($7319)
JH Football	John Greaney	($4719)
Varsity Golf	Mike Sinclair	($5738)
JV Golf	Stephen Edmonds	($4900)
Varsity Gymnastics	Steve Silipo	($7361)
Assistant Varsity Gymnastics	Nancy O'Donnell	($5820)
Varsity Boys Soccer	Dennis McGovern	($5720)
Assistant Varsity Boys Soccer	Kyle Cropsey	($4900)
JV Boys Soccer	Michael Birnbaum	($4900)
JH Boys Soccer	Jeff Kenney	($4719)
JH Boys Soccer	Alex Marange	($4719)
Varsity Girls Soccer	Frank Mancuso	($5720)
Assistant Varsity Girls Soccer	Melissa Pascarella	($4900)
JV Girls Soccer	Edward Aromando	($4900)
JH Girls Soccer	Nicole Blair	($4719)
JH Girls Soccer	Katie Marmo	($4719)
Varsity Girls Tennis	Rob Andrews	($5738)
JV Girls Tennis	Lauren Heck	($4900)
JH Girls Tennis	Rich Villanueva	($4719)
Varsity Girls Volleyball	Lauren Halverson	($7361)
JV Volleyball	Brenda Mayo	($5820)
Girls Swimming (Supervisor)	Stephanie Greaney	($1015)
Fall Weight Room Supervision	Danny McHugh	($1015)
Athletic Trainer	Professional PT Contract	

7. **CASUAL APPOINTMENT: RESOLVED,** that the Board of Education appoints Stephanie Greaney as the Individual Competitor Swimming Supervisor for Babylon students who practice with the West Islip Swim Team, West Islip Swim Club, and **BE IT FURTHER RESOLVED,** that the Board of Education authorizes the West Islip Swim Team appointed coach, Tanya Carbone (girls) Thomas Loudon (boys), West Islip Swim Club, Kerri Whalen-Mitchell, to coach Babylon Students. Compensation for Richard Villanueva to be at the current supervision rate of pay for the 2020-2021 school year.

8. **CASUAL APPOINTMENTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following casual appointments from September 1, 2020 to June 30, 2021. Compensation for these position to be in accordance with the 2020-2021 Babylon Teachers' Association Contract.

7-12 Technology Director	Steve Silipo	($9214)
7-12 Dean of Discipline	Michael Collins	($9214)
Administrative Assistant (HS)	Philip Grande	($8274)

9. **CASUAL APPOINTMENT: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following administrative casual appointments for the Summer Programs from July 6, 2020 to August 14, 2020. Compensation for these positions to be a stipend of $3,000 each.

Co-Principal	Lisa Consolo
Co-Principal	Lauren Fretto

10. **CASUAL APPOINTMENTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following casual appointments for the K-6 Summer Skills Program from July 6, 2020 to August 14, 2020. Compensation for these positions to be in accordance with the 2020-2021 Babylon Teachers' Association Contract at $45.50/hour.

Kindergarten	Brianna Mullady
	Lindsay Carbone
First Grade	Megan Connolly
	Jennifer Rummel
Second Grade	Olivia Aebli
	Caroline Figoski
Third Grade	Ashley Belmonte
	Samantha Czeczotka
Fourth Grade	Kelly Arcoleo
	Kim Gentile
Fifth Grade	Nicole Cupo
	Steve Fasciani
Sixth Grade	Jessica Kurtz
	Jacie Chatterton

11. **CASUAL APPOINTMENTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following casual appointments for the Extended School Year Program from July 6, 2020 to August 14, 2020. Compensation for these positions to be in accordance with the 2020-2021 Babylon Teachers' Association Contract at $45.50/hour and aides and monitors agreement at the hourly rates of Step 2-$18.20, Step 3-$18.55

Teachers:	Lindsay Carbone
	Nicole Cupo
	Keith Fasano
	Denise Glynn
	Barbara O'Halloran
	Robin LaBarbera
	Eileen Ratto
	Caroline Figoski
Nurse	Nina Burke
Nurse substitute	Grace McHugh
Aides	Claire Joseph
	Karen Altieri
	Jean Marie Flaugher
	Heather Tenety
	Maria Gangone
	Ellen Altieri

12. **CASUAL APPOINTMENTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the following casual appointments from September 1, 2020 to June 30, 2023. Compensation for these positions to be in accordance with the Babylon Teachers' Association Contract ($9214)

7-12 Science Director	Melissa Callahan
7-12 English Director	Teresa Collins
7-12 Special Education Director	Stephen Vaccaro

13. **RECLASSIFICATION CIVIL SERVICE TITLE: RESOLVED,** that upon the recommendation of the Superintendent of Schools, and as a result of the Suffolk County Civil Service review, the Board of Education approves the reclassification of Theresa Pluschau from Senior Account Clerk to Principal Account Clerk effective July 1, 2020. Compensation for this appointment to be Column A/Step 8 of the 2020-2021 CSEA Clerical/Nursing/Network & Systems Technicians Association contract. ($65,806)

14. **NON-UNION PERSONNEL: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education hereby approves the salaries and fringe benefit agreement for Kevin Warren, Director of Facilities III, Linda Pesce, Secretary to the Superintendent/Assistant Superintendent/District Clerk, Donna Lika, Sr. Account Clerk/District Treasurer, and Charles Dwyer, Network & Systems Administrator, as approved in the 2020-2021 school budget covering the period July 1, 2020-June 30, 2021.

15. **APPROVAL FOR NIGHT AND WEEKEND DIFFERENTIAL: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the night and weekend differential for the following buildings and grounds staff for the 2020-2021 school year. Compensation to be in accordance with the 2020-2021 CSEA Custodial Agreement.
    Night Differential: Lisa Brunjes, James Lind, William Rivas, Joseph Jones, David Marcopoulos, Stephen DeRusso, Brigida Berroa, Gayle McGuickian, Bernadita Rodriguez ($1462.00)
    Weekend Differential: Stephen DeRusso, Joseph Loudon ($1232.00)

16. **FIRST READING OF POLICIES: RESOLVED,** that upon the recommendation of the Superintendent of Schools the Board of Education conducts a first reading of the following policies: 4526/Computer Network Use, 4526-R/Regulation for Computer Network Use, 4526-E.2/Computer Network Use Regulation Exhibit, 4526.1/Internet Safety, 4526.4/Student Email Accounts and Communication, 8635/Information and Data Privacy Security, Breach and Notification, 8635-R/Information and Data Privacy, Security, Breach and Notification Regulation, and 8635-E/Parent's Bill of Rights for Student Data Privacy & Security and BE IT FURTHER RESOLVED, that the Board of Education waives the formal first reading of policies 4526/Computer Network Use, 4526-R/Regulation for Computer Network Use, 4526-E.2/Computer Network Use Regulation Exhibit, 4526.1/Internet Safety, 4526.4/Student Email Accounts and Communication, 8635/Information and Data Privacy Security, Breach and Notification, 8635-R/Information and Data Privacy, Security, Breach and Notification Regulation, and 8635-E/Parent's Bill of Rights for Student Data Privacy & Security, as attached.

17. **LONG ISLAND SCHOOL NUTRITION DIRECTORS COOPERATIVE BID: WHEREAS,** it is the plan of a number of public school districts in Nassau/Suffolk Counties, New York, to bid jointly on selected Food Service Commodities, Food and Food Service Supplies for the 2020-2021 school year. **WHEREAS,** Babylon Union Free School District is desirous of participating with other districts in Nassau/Suffolk Counties in the joint bidding of the commodities mentioned above as authorized by General Municipal Law, Section 119-0, and **WHEREAS,** Babylon Union Free School District wishes to appoint a committee to assume the responsibility of drafting specification, advertising for bids, accepting and opening bids, reporting the results to the Boards of Education and making recommendations thereon; therefore, **BE IT RESOLVED,** that the Board of Education of the Babylon Union Free School District, hereby appoints Long Island School Nutrition Directors Association Cooperative Bid Committee to represent it in all matters related above, and **BE IT FURTHER RESOLVED,** that the Babylon Union Free School District's Board of Education authorized the above mentioned committee to represent it in all matters leading up to the entering into a contract for the purchase of the above mentioned commodities, and **BE IT FURTHER RESOLVED,** that the Babylon Union Free School District's Board of Education agrees to assume its equitable share of the costs of the cooperative bidding, and **BE IT FURTHER RESOLVED,** that the Babylon Union Free School District's Board of Education agrees 1) to abide by the majority decisions of the participating districts on quality standards; 2) that unless all bids are rejected, it will award contracts according to the recommendations of the committee; 3) that after award of contract(s) it will conduct all negotiations directly with the successful bidder(s).

18. **NEW TEXTBOOK ADOPTION: RESOLVED,** that upon the recommendation of the Superintendent of Schools the Board of Education adopts the following textbook: Krugman's Macroeconomics for the AP Course, Co-authored by David Anderson of Centre College and Margaret Ray of University of Mary Washington. Published by Bedford, Freeman & Worth

19. **REORGANIZATION MEETING/REGULAR BUSINESS MEETING: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Reorganization Meeting of the Board of Education of the Babylon Union Free School District be scheduled for 7:00 p.m. on Tuesday, July 7, 2020 and **BE IT FURTHER RESOLVED,** that the Regular Business Meeting of the Board of Education of the Babylon UFSD be held immediately following the Reorganization Meeting on July 7, 2020.

20. **CONSULTANT SERVICES AGREEMENT: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the consultant services agreement between the Babylon UFSD and Anthony Ciervo effective July 1, 2020 to June 30, 2021. Compensation to be on days specifically requested at a rate of $500.00/day.

21. **GUERCIO & GUERCIO CONTRACTS: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education authorizes the President of the Board of Education to execute a contract between the Babylon Union Free School District and Guercio & Guercio for the General Counsel Contract and Labor Counsel Contract from July 1, 2020 to June 30, 2021, fee structure as per contract.

22. **SPECIAL EDUCATION CONSULTANT SERVICES CONTRACT: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the Board of Education approves the special education consultant services contract for the 2020-2021 school year between the Babylon UFSD and Beyond Boundaries Autism Specialists Applied Behavior Analysis, PLLC (SECSC 2020-2021 #16), The Long Island Home, dba South Oaks Hospital (SECSC-2020/2021 #9), Access 7 Services, Inc. (SECSC 2020/2021 #17).

23. **COMMITTEE ON SPECIAL EDUCATION AND COMMITTEE ON PRESCHOOL EDUCATION: RESOLVED,** that upon the recommendation of the Superintendent of Schools, the recommendations from the Committee on Special Education and Committee on Preschool Special Education for cases from December 16, 2019 through June 11, 2020 be accepted.

IX. Other Business

X. Representatives of Organizations

XI. Questions from Visitors can be emailed in advance by 3:00 p.m. on June 22, 2020 to babylonschools@babylonufsd.com

XII. Future Board Meetings: Reorganization/Regular Business Meeting
Tuesday, July 7, 2020

XIII. Adjournment

COMPUTER NETWORK USE

The Board of Education is committed to optimizing student learning and teaching. The Board considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in district classrooms solely for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning and can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

All users of the district's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility.

The Superintendent of Schools shall establish regulations governing the use and security of the district's computer network. All users of the district's computer network and equipment shall comply with this policy and those regulations. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent shall be responsible for designating a District Director of Technology & Accountability and a Network Administrator to oversee the use of district computer resources. The District Director of Technology & Accountability shall be the Director of the Office of Technology & Accountability. The Assistant Superintendent for Curriculum and Instruction will prepare in-service programs for the training and development of district staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent, working in conjunction with the Deputy Superintendent, the District Director of Technology & Accountability, the Network Administrator and the Assistant Superintendent for Curriculum and Instruction will be responsible for the purchase and distribution of computer software and hardware throughout district schools.

Adoption date: November 13, 2007
Revised: October 19, 2009
Re-Adoption date:

REGULATION FOR COMPUTER NETWORK USE POLICY

The following rules and regulations govern the use of the district's technology and network including access to the Internet.

I. Network and Technology Administration

- The Superintendent of Schools shall designate a District Director of Technology & Accountability to oversee the district's technology and network.
- The District Director of Technology & Accountability shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The District Director of Technology & Accountability shall be responsible for supporting district policy and regulations governing use of the district's network at the building level with all network users.
- The Assistant Superintendent for Curriculum and Instruction and the District Director of Technology & Accountability shall provide employee training for proper use of the network. Staff supervising students using the district's network, in turn, will provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- The District Director of Technology & Accountability shall ensure that all software installed on the network has been properly purchased and licensed to the district or work in conjunction with special education on "Assistive Technology" installations and scanning for computer viruses.
- The District Director of Technology & Accountability shall maintain the district instructional technology inventory.
- The District Director of Technology & Accountability shall be responsible for the administration and integrity of the active directory and group policies.
- The District Director of Technology & Accountability shall be a part of all planning projects for any technology installations.
- The District Director of Technology & Accountability shall review and maintain Internet filters for violations or inappropriate access by users.
- Only hardware (computers, tablets, printers, workstations, servers, routers, network switches, etc.) purchased, managed and maintained by the Office of Technology & Accountability will be permitted on the district network. Personal hardware (consumer printers, computers, laptops, routers, etc.) will not be maintained nor added to the district's network. Faculty and guests may add personal laptops, tablets, and other devices to the wireless network using the instructions provided by the Office of Technology & Accountability.
- District faculty and staff are prohibited from purchasing and/or receiving (through donation, grant or loan) technology (hardware and software) without the involvement of and written permission from the Office of Technology & Accountability.
- This includes but is not limited to any software, programs, computers, laptops, printers, servers, routers, switches, tablets, iPads, or any other hardware requiring district support.
- All Student agreements to abide by district policy and regulations, parental consent forms, and 1:1 device procedures. 1:1 device insurance coverage election form will be kept in the Office of Technology & Accountability.

II. Internet Access

- Internet access is a privilege and may be revoked for misuse, malicious use, bullying or any infraction against the District's Technology Policies, including but not limited to Policy 4526, Regulation 4526-R, Regulation 4526.1-R, Policy 4526.4, Policy 8635, Policy 8635-R, and all other District policies governing the use of information technology in the District, and or Code of Conduct.
- All staff and students will be provided with a district network account.
- Internet access is for educational and administrative purposes only.
- Internet access is restricted depending on the filtering level of the user.
- The district network is the only acceptable medium for Internet access for educational purposes and/or official school business.
- Cyberbullying, social network sites (such as Facebook, Instagram, Pinterest, Tumblr, Reddit, Twitter, Google+, Vine, Snapchat, KiK, YikYak, WhatsApp, Tinder, etc.) that cannot be filtered for inappropriate material are strictly prohibited at all times on the district's network except by authorized district administration for investigative purposes.
- The district offers YouTube filtering to allow appropriate educational material at the teachers request.
- All faculty and staff will be filtered by the district's Internet filter. In the event a teacher or class wishes to do research or work outside of the filter they will need to request permission to bypass the filter for a specific topic and/or site.
- District devices (purchased by the district through the Office of Technology and Accountability will automatically receive Internet/wireless access. Staff may add personal devices or non-district purchased devices to the wireless network with approval from the Office of Technology & Accountability.

III. Acceptable Use and Conduct

- Access to the district's technology is provided for educational or administrative purposes and/or for research consistent with the district's mission and goals.
- Use of the district's technology is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Staff and students will never share their personal network credentials or any district usernames/passwords with anyone at any time. All network users are expected to abide by the generally accepted rules of network etiquette (netiquette). This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and obscenities are all strictly prohibited.
- Network users identifying a security problem on the district's network must notify the Administrator for Information Technology. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.
- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.
- Teachers and parents have received copies of the District's e-mail guidelines.

IV. Procedures for Proper Use

The following guidelines govern proper use of all district technology.

- The individual in whose name an account is issued is responsible at all times for its proper use.
- Network users will be issued a login name and password. Passwords must be changed periodically. Passwords must follow the guidelines issued by the Office of Technology & Accountability.
- Only approved software, extension and/or apps (purchased and licensed to the district) will be installed on any district computer, laptop, tablet, mobile device. Under no circumstances will personal, unlicensed, or unauthorized software be installed on district computers (this includes district laptops, tablets and other devices).
- Do not leave the account open and unattended.
- Always log off or log out when leaving a computer.
- Other than the Office of Technology & Accountability or a member of the IT Staff, no users will have any installation rights on any school district computer (this includes school owned laptops and mobile tablets).

V. Prohibited Activity and Uses

The following is a list of prohibited activity concerning use of the district's technology. Violation of any of these prohibitions may result in disciplinary or other appropriate penalty.

- Using the network for commercial activity, including advertising. This includes solicitation for non-district sanctioned events, products, services or propaganda using the district email system, website or any other technical resources.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Using the network for any act of bullying or DASA infraction.
- Using another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.

- Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Violations of students/staff rights as per the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA) and/or the Children's Internet Protection Act (CIPA).
- Using the network for sending and/or receiving personal messages either to an excessive degree and/or in a manner inappropriate for a professional and educational environment.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the district's computers and/or network
- Using district technology resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Unauthorized file sharing, piracy, or torrent downloading, including the unlawful exchange of copyrighted media, software, or related materials.
- Gaining or seeking to gain unauthorized access to any district technology resources, or vandalizing the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Privately licensed streaming services (Netflix, Amazon Prime, iTunes Music/Movies, Hulu, Showtime, HBO, Starz, etc.) are strictly prohibited for use in education as these services are not under the "Fair Use" law as per the individual license agreements between individual user and service. These copyrighted broadcasts may not be used in public and educational settings and therefore are strictly prohibited on the district network.
- Purchase or receipt of hardware (computers, tablets, printers, workstations, servers, routers, network switches, etc.) without the authorization of the Office of Technology & Accountability. Only hardware purchased, managed and maintained by the Office of Information Technology & Accountability will be permitted on the district network. Personal hardware (consumer printers, computers, laptops, routers, etc.) will not be maintained nor added to the district's network. Faculty may add personal laptops, tablets, devices to the wireless network using the instructions provided by Office of Technology & Accountability.

VI. No Privacy Guarantee

All users using the district's technology should not expect, nor does the district guarantee privacy for electronic mail (e-mail) or any use of the district's technology. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's technology.

VII. Sanctions

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

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 materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

VIII. District Responsibilities

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's computer network and the Internet use these information technologies and services at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: November 13, 2007
Revised date: October 19, 2009
Re-Adoption date:

COMPUTER NETWORK USE REGULATION
EXHIBIT

Staff Agreement Form

You have requested access to the Babylon Union Free School District Computer Network. This access includes the use of district-owned hardware, software and connections to computers through the Internet, which would connect you with educational resources worldwide. In accepting an account, you accept the responsibility of using the network and related resources in an appropriate manner.

Please read the Computer Network Use Regulation *(4526-R)* and complete this form to indicate that you agree to terms and conditions outlined.

As an employee of the Babylon Union Free School District and a user of the computer network, I acknowledge receipt of the Computer Network Use Regulation.

Signature:_____ Date:_____

Name (Please Print): _____

Primary Work Location: _____

Job Title: _____

Home Address: _____

Home Telephone:_____ Day Telephone: _____

Please complete this form and return same to the Office of Technology & Accountability, prior to being given your network ID and initial logon password.

Adoption date: June 10, 2002
Revisited date: October 19, 2009
Re-Adoption date:

STUDENT EMAIL ACCOUNTS AND COMMUNICATION

Student email can be a powerful communication tool for students to increase communication and collaboration. Students are encouraged to check their email at least once per day. Teachers may send email to grade school and Jr.-Sr. high school students to communicate reminders, course content, pose questions related to class work, and such. Students may send email to their teachers with questions or comments regarding class. Students may send email to other students to collaborate on group projects and assist with school classes. Students are encouraged to email staff concerning school-related content and questions. However, there will be no requirement or expectation for staff to answer student email outside of their regular workday, although they certainly may if they choose. For example, an unanswered email to a teacher would not excuse a student from turning in an assignment.

The management of student email account access is critical to ensure safety, high quality and proper use of the system. The student email account management will be accomplished through the Office of Technology & Accountability and managed by the District Director of Technology & Accountability. Students are bound to all of the rules and regulations set forth in the Regulation for District Technology (4526-R), Prohibition of Cyberbullying and Harassment Policy (4526.3), the Code of Conduct (5300), as well as the additional provisions below. Students who violate any of these policies may be subject to revocation of their privileges and may face disciplinary actions as deemed fit by the Principal or Office of Technology & Accountability .

Procedures for Proper Use and Acceptable Use Conduct

- All student email accounts are property of the Babylon School District. Email activities must comply with all of the District's Technology Policies, including but not limited to Policy 4526, Regulation 4526-R, Regulation 4526.1-R, Policy 4526.4, Policy 8635, Policy 8635-R, and all other District policies governing the use of information technology in the District. The users of student email accounts are to be deemed for all purposes knowledgeable of this policy.
- All student email will reside on the District's Microsoft Office 365 server managed through the Active Directory and maintained by the Office of Technology & Accountability. Students are not permitted to use any other email accounts (i.e. Yahoo, Hotmail, AOL, Gmail, etc.) as official district email accounts or to communicate with faculty and staff.

- For the protection of our students and their own protection, administration, faculty and staff will only use their official district email address to email students at their official district email address and not side-step district security using personal or outside email communication (i.e. Yahoo, Hotmail, AOL, Gmail, etc.).
- The student will be removed from the system after graduation, leaving the school district, or revocation of privileges due to any policy infractions.
- Messages posted on the district's email system cannot cause disruption to the school environment or normal and acceptable school operations.
- The email system cannot be used to operate a personal business. The account may not be sold or otherwise reassigned. The account may be revoked if used inappropriately.
- Students will report any unusual activities such as inappropriate communications, obscene email, attempts by adults to lure them into dangerous behaviors, and the like to a faculty member or Principal.
- Students will not identify their home telephone numbers, or home addresses in any email correspondence.
- Email sent or received by the district email system is not confidential. Although the Board of Education does not make a practice of monitoring email, the administration reserves the right to retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages, to conduct internal investigations, to comply with investigations of wrongful acts or to recover from system failure.
- When issues arise, the Office of Technology & Accountability will deal directly with the school administration. The school administration will deal directly with the student and/or parents/guardians. Improper use of the system will result in discipline and possible revocation of the student email account. Illegal activities on the system will be referred to law enforcement authorities for appropriate legal action.
- Students will only have the capability of sending/receiving email to/from district email accounts (administrators, teachers, staff, other students) at the @babylonufsd.com. Student email accounts will not be able to send to or receive from any other domain or account. The Office of Technology & Accountability will work towards, a monitored system, for high school juniors and seniors, to have the capabilities of emailing external accounts for the purpose of college admissions (i.e. .educational accounts).
- The Office of Technology & Accountability will work towards, a monitored system, with other departments in order to whitelist specific email addresses that are relevant to instructional programs for Jr.-Sr. High school students.
- Students may not forward email to their personal or outside account and will only have the ability to communicate within the babylonufsd.com domain.
- If necessary, the Board of Education, at its discretion, may close the accounts at any time. Any updates or changes to this email policy by the Board of Education or administration will be in effect.

Cross-ref: 4526, Policy for District Technology
4526-R, Regulation for District Technology Acceptable Use Policy
4526.3. Prohibition of Cyberbullying and Harassment
5300. Code of Conduct

Adoption date:

INTERNET SAFETY

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access:

- For adults: visual depictions that are obscene or represent child pornography, and
- For minors: visual depictions that are obscene, represent child pornography, or are harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The District Director of Technology & Accountability designated under the district's policy on the acceptable use of district computers (policy 4526) shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. The District Director of Technology & Accountability shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's policy on the acceptable use of computers and the internet (policy 4526). Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

As part of this policy, and the district's policy on acceptable use of district computers (policy 4526), the district shall also provide age-appropriate instruction regarding appropriate online behavior, including:

1. interacting with other individuals on social networking sites and in chat rooms, and
2. cyberbullying awareness and response.

Instruction will be provided even if the district prohibits students from accessing social networking sites or chat rooms on district computers.

Cross-ref: 4526. Computer Use in Instruction

Ref: Children's Internet Protection Act. Public Law No. 106-554
Broadband Data Services Improvement Act/ Protecting Children in the 21st Century Act, Public Law No. 110-385
47 USC §254
20 USC §6777

Adoption date: November 9, 2009
Re-Adoption Date:

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Protection Officer (DPO) is responsible for ensuring the district's systems follow NIST CSF and working with the Office of Technology & Accountability adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy. This appointment will be made at the annual organizational meeting.

The Board directs the Superintendent of Schools. in accordance with appropriate business and technology personnel, and the Data Protection Officer (where applicable) to establish regulations which address:

- the protections of "personally identifiable information" of student and teachers/principal under Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

1. Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

A. General Provisions

Personally Identifiable Information, ("PII"), as applied to student data, is as defined in the Family Educational Rights and Privacy Act (Policy 5500), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. The term PII, as applied to teacher and principal data, means the results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of PII by the district benefits students and the district (e.g., improve academic achievement, empower parents and students

with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents.

The district will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry stand ard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

Under no circumstances will the district sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the district will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the district will not report the following student data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The district has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the district's website at www.babylonufsd.com and can be requested from the district clerk.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):

   a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
   b. unless required by statute or court order and the third party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If any third-party contractor has a breach or unauthorized release of PII, it will promptly notify the district in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must be accepted by the district.

At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of the Rules of the Commissioner of Education;
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district;
7. describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

The district will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII. The District Director of Technology & Accountability shall be responsible for implementing this training program. The training

program shall include instructions on uniform procedures for staff to follow in the event of a PII breach or unauthorized disclosure. Such training shall instruct staff that complaints regarding any issue related to PII may be reported to the Data ProtectionOfficer, and, further, that any District employee who receives such a complaint must immediately report it to the Data Protection Officer.

E. Reporting

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

The district will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, the district will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied, or the risk of interference with the law enforcement investigation ends.

The Superintendent, in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

II. "Private Information" under State Technology Law §208

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the district must be promptly reported to the Superintendent and the Board of Education.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email address;
4. Internet identification name or password;
5. parent's surname prior to marriage; and
6. drivers' license number.

In addition, the district will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref:
1120, District Records
5500, Student Records

Ref:
State Technology Law §§201-208
Labor Law §203-d
Education Law §2-d
8 NYCRR Part 121

Adoption Date:

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION REGULATION

The district will inventory its computer programs and electronic files to determine the types of information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

I. Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

A. Definitions

"*Biometric record*," as applied to student Personally Identifiable Information (PII), means one or more measurable biological or behavioral characteristics that can be used for automated recognition of persons, which includes fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

"*Breach*" means the unauthorized acquisition, access, use, or disclosure of student PII and/or teacher or principal PII by or to a person not authorized to acquire, access, use, or receive the student and/or teacher or principal PII.

"*Disclose*" *or Disclosure* mean to permit access to, or the release, transfer, or other communication of PII by any means, including oral, written, or electronic, whether intended or unintended.

"*Personally Identifiable Information*" (PII) as applied to students means the following information for district students:

1. the student's name;
2. the name of the student's parent or other family members;
3. the address of the student or student's family;
4. a personal identifier, such as the student's social security number, student number, or biometric record;
5. other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
7. information requested by a person who the district reasonably believes knows the identity of the student to whom the education record relates.

"*Personally Identifiable Information*" (PII) as applied to teachers and principals means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

"*Third-Party Contractor*" means any person or entity, other than an educational agency (i.e., a school, school district, BOCES or State Education Department), that receives student or teacher/principal PII from the educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This includes an educational partnership organization that transmits and receives student and/or teacher/principal PII from a school district to carry out its responsibilities pursuant to Education Law §211-e (for persistently lowest-achieving schools or schools under registration review) and is not an educational agency. This also includes a not-for-profit corporation or other nonprofit organization, other than an educational agency.

B. Complaints of Breaches or Unauthorized Releases of PII

If a parent/guardian, eligible student, teacher, principal or other district employee believes or has evidence that student or teacher/principal PII has been breached or released without authorization, such person must submit a complaint in writing to the district. Complaints may be received by the Data Protection officer, but may also be received by any district employee, who must immediately notify the Data Protection Officer. This complaint process will be communicated to parents, eligible students, teachers, principals, and other district employees.

The district will acknowledge receipt of complaints promptly, commence an investigation, and take the necessary precautions to protect personally identifiable information.

Following its investigation of the complaint, the district will provide the individual who filed a complaint with its findings within a reasonable period of time. This period of time will be no more than 60 calendar days from the receipt of the complaint.

If the district requires additional time, or if the response may compromise security or impede a law enforcement investigation, the district will provide the individual who filed a complaint with a written explanation that includes the approximate date when the district will respond to the complaint.

The district will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.

C. Notification of Student and Teacher/Principal PII Breaches

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the Data Protection Officer in the most expedient way possible, without unreasonable delay, but no more than seven calendar days after the breach's discovery.

The Data Protection Officer will then notify the State Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the State Education Department.

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

The district will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, the district will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a brief description of the breach or unauthorized release,
- the dates of the incident and the date of discovery, if known;
- a description of the types of PII affected;
- an estimate of the number of records affected;
- a brief description of the district's investigation or plan to investigate; and
- contact information for representatives who can assist parents or eligible students with additional questions.

Notification must be directly provided to the affected parent, eligible student, teacher or principal by first-class mail to their last known address; by email; or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor will pay for or promptly reimburse the district for the full cost of such notification.

The unauthorized acquisition of student social security numbers, student ID numbers, or biometric records, when in combination with personal information such as names or other identifiers, may also constitute a breach under State Technology Law §208 if the information is not encrypted, and the acquisition compromises the security, confidentiality, or integrity of personal information maintained by the district. In that event, the district is not required to notify affected people twice, but must follow the procedures to notify state agencies under State Technology Law §208 outlined in section II of this regulation.

II. "Private Information" under State Technology Law §208

A. Definitions

"*Private information*" means either:

1. personal information - consisting of any information in combination with any one or more of the following data elements, when either the data element or the personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:
   - Social security number;
   - Driver's license number or non-driver identification card number:
   - Account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account:
   - account number or credit or debit card number, if that number could be used to access a person's financial account without other information such as a password or code; or
   - biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, or retina or iris image) used to authenticate or ascertain a person's identity; or

2. a user name or email address, along with a password, or security question and answer, that would permit access to an online account.

"Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

"*Breach of the security of the system*" means unauthorized acquisition or acquisition without valid authorization of physical or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district. Good faith acquisition of personal information by an officer or employee or agent of the district for the purposes of the district is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

B. Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district will consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as the removal of a lost or stolen computer, or other device containing information:
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and or
4. any other factors which the district shall deem appropriate and relevant to such determination.

C. Notification of Breaches to Affected Persons

Once it has been determined that a security breach has occurred, the Data Protection Officer will take the following steps:

1. If the breach involved computerized data *owned or licensed* by the district, the district will notify those New York State residents whose private information was, or is reasonably believed to have been accessed or acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the system. The district will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures.
2. If the breach involved computer data *maintained* by the district, the district will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization.

The required notice will include (a) district contact information, (b) a description of the categories of information that were or are reasonably believed to have been accessed or acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention. This notice will be directly provided to the affected individuals by any of the following means:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of each such electronic notification. In no case, however, will the district require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
3. Telephone notification, provided that the district keeps a log of each such telephone notification.

However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the district has such address for the affected individual;
2. Conspicuous posting on the district's website, if they maintain one; and
3. Notification to major media.

However, the district is not required to notify individuals if the breach was inadvertently made by individuals authorized to access the information, and the district reasonably determines the breach will not result in misuse of the information, or financial or emotional harm to the affected persons. The district will document its determination in writing and maintain it for at least five years, and will send it to the State Attorney General within ten days of making the determination.

Additionally, if the district has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d, it is not required to notify them again. Notification to state and other agencies is still required.

D. Notification to State Agencies and Other Entities

Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the district will also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

If the district is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the State Attorney General within five business days of notifying the Secretary.

Adoption Date:

Parent's Bill of Rights for Student Data Privacy & Security

The Babylon Union Free School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Babylon Union Free School District establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov.data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to: Babylon UFSD – Attn: Data Protection Officer, 50 Railroad Avenue, Babylon, NY 11702
- Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII

- In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting Data Protection Officer, 50 Railroad Avenue, Babylon, NY 11702, 631-893-7983, or can access the information on the district's website at www.babylonufsd.com.

PARENT BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY THIRD PARTY CONTRACTOR SUPPLEMENT

The **Company Name** has been engaged by the Babylon UFSD to provide services. In this capacity, the company may collect, process, manage, store or analyze student or teacher/principal personally identifiable information (PII). ***Company Name*** Data Privacy and Security Plan is as follows:

Company Name acknowledges that it has the following obligations under New York Education Law § 2-d with respect to student data received from Babylon UFSD, and agrees that any failure to fulfill one or more of these statutory obligations shall be deemed a breach of the Agreement between ***Company Name*** and Babylon UFSD (as well as subject ***Company Name*** to various penalties under section 2-d, including but not limited to civil penalties). ***Company Name*** acknowledges the provisions of the Babylon UFSD Parents' Bill of Rights, which it incorporates into this security and privacy plan as Section 2.

Student Data and Commitment to Data Security
Please outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with NYS Ed Law 2-d, and demonstrate that it complies with the requirements of Section 121.3(c) of the Regulations of the Commissioner of Education;

Employee and Subcontractor Privacy Policy
Please specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access. Please also specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.

Physical Safeguards
Please describe the location and manner that protects data security and please specify the safeguards and practices it has in place to protect PII. Please include the following:

- *Password protections*
- *Administrative procedures*
- *Encryption while PII is in motion and at rest*
- *Firewalls*

Data Breaches

Please specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district.

Provisions upon Expiration of Agreement

Please describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

Privacy Contact Information

Parents may challenge the accuracy of PII held by **Company Name** by contacting:
Name:
By e-mail:
By Phone:

The contractor's agreement with the district begins on (*insert date*) and ends on (*insert date*). Once the contractor has completed its service to the district, records containing student PII will be (*select one*: destroyed or returned) by (*insert date*) via the following (insert method if destroyed or format if returned).

Adoption date: