Privacy Officer

We will designate a Privacy Officer for the Plan and the Board in writing. The Privacy Officer shall be responsible for developing and implementing our privacy policies and procedures that relate to PHI, including without limitation, those set forth in these Policies.

The Privacy Officer will be listed in the Board's telephone directory and its website www.wallingford.k12.ct.us.

The Privacy Officer shall be responsible for, among other things:

1. Implementing, administering and updating privacy policies and procedures to ensure compliance with the standards, implementation specifications and other requirements of HIPAA and other applicable laws;

2. Coordinating privacy and individual rights issues with the Plan's third party administrator and ensuring that all third party administrators commit to hold PHI received on behalf of the Plan in accordance with the requirements of HIPAA and other applicable laws;

3. Developing, maintaining and updating the privacy forms required by these Policies and HIPAA and other applicable laws;

4. Arranging for and documenting the training of the Board's Authorized Employees on privacy policies and procedures and the requirements of HIPAA and other applicable laws;

5. Establishing and maintaining organized files and records of privacy policies and practices and retaining such files and records in accordance with HIPAA and other applicable laws;

6. Receiving and investigating complaints about violations of our privacy policies or HIPAA and other applicable laws; and

7. Serving as the contact person for Plan Participants who have questions, concerns or complaints about the privacy of their PHI.

I. Training

The Board will provide training regarding these Policies to its Authorized Employees who have access to PHI in connection with the Plan. This training will include, at a minimum, information regarding permissible and impermissible uses and disclosures of such PHI and the procedures for filing complaints for violations of privacy laws and policies.

Privacy Officer (continued)

For Authorized Employees who receive PHI in connection with the Plan, successful completion of these training sessions is a prerequisite to continued employment and failing to attend scheduled training sessions may result in disciplinary consequences.

II. Safeguards and Firewalls

The Board will establish appropriate technical and physical safeguards to prevent any PHI that it may receive in performing administrative functions on behalf of the Plan from intentionally or unintentionally being used or disclosed in violation of HIPAA. Technical safeguards include limiting access to information by creating computer firewalls and physical safeguards such as locking doors or filing cabinets. Firewalls shall be adequate to ensure that only Authorized Employees will have access to PHI, and only for plan administrative purposes, and that any other employees of the Board will not have access to PHI.

III. Complaints about Privacy Issues

The Privacy Officer will be the Plan's contact person for receiving complaints. The Privacy Officer will investigate such complaints as promptly as possible under the circumstances and will recommend corrective action where appropriate.

Any employee or other individual who becomes aware of any violation of the privacy laws or the policies or who wishes to complain about the policies and procedures shall promptly report such matter to the Privacy Officer. Each complaint shall be submitted in writing, either on paper or electronically, and shall describe the specific conduct or policies that are the subject of the complaint. A complaint may initially be made orally but must be followed within five (5) business days by a written complaint as described above.

The Privacy Officer or his or her designee shall maintain a record of all privacy complaints received and the disposition of such complaints and such records shall be retained for a period of at least six (6) years from the date of the complaint.

IV. Sanctions

Authorized Employees who have access to PHI in connection with plan administrative functions will be subject to appropriate sanctions, including termination of employment, if they fail to comply with these Policies or applicable privacy laws. In addition, employees may be subject to both civil and criminal penalties for violation of privacy laws and may be sued by aggrieved individuals seeking damages for unauthorized or improper use or disclosure of PHI.

Privacy Officer (continued)

V. Mitigation of Inadvertent Uses or Disclosures of PHI

We will take all necessary and appropriate steps to mitigate, to the extent possible, any harmful effects that become known as a result of the unauthorized use or disclosure of a Plan Participant's PHI in violation of these Policies. Any unauthorized or improper use or release of PHI should be reported immediately to the Privacy Officer.

The Privacy Officer shall develop a plan for mitigating the effects of any known instance of unauthorized use or disclosure of PHI and shall be responsible for implementing such plan and reporting to the Superintendent, or his or her designee, on such mitigation efforts. Where appropriate, the Privacy Officer shall consult with legal counsel regarding appropriate steps to be taken to mitigate any harmful effects of such unauthorized use or disclosure.

VI. No Intimidation or Retaliatory Acts; No Waiver of Rights

No Plan Participant shall be subject to any intimidation, threats, reprisals, coercion, discrimination or other retaliatory actions for (i) exercising any right under these Policies or applicable law, (ii) filing any privacy complaint with the Privacy Officer, the third party administrator, or the Secretary of HHS, (iii) testifying, assisting or participating in any investigation or other proceeding relating to these privacy policies or applicable privacy laws, or (iv) opposing any acts or practices that are in violation of these policies or are unlawful, provided that such individual has a good faith belief that the practice that is being opposed is a violation of these policies or is unlawful, and the manner of the opposition is reasonable and does not involve the unlawful disclosure of PHI.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility under any of the Plan.

VII. Documentation

Any documentation created or received by us in connection with protecting the privacy of PHI and the rights of Plan Participants with respect to PHI shall be retained by us for at least six years from the date that such documentation was either created or last given effect, whichever is later. By way of example, this retention standard shall apply to these Policies, our Notice of Privacy Practices, authorizations by Plan Participants, business associate contracts, the identity of individuals responsible for processing requests from Plan Participants to access, amend or receive an accounting of PHI, designation of the Privacy Officer, documentation of additional restrictions for a Plan Participant's PHI, documentation of complaints, and other items requiring documentation under applicable privacy laws. Such documentation may be retained in either paper or electronic form.

Privacy Officer (continued)

VII. Documentation (continued)

Any changes to our policies and procedures with respect to HIPAA Privacy compliance must be reduced to writing and documented through an amendment to these Policies, and, if appropriate, indicated in a revised Notice of Privacy Practices. Additionally, the list, by name, title or class, of Authorized Employees (those employees of the Board who are authorized to receive PHI for the performance of administrative functions on behalf of the Plan) shall be documented in the Plan Amendment. Any changes to such list of Authorized Employees shall be made through a further amendment to the Plan Amendment. Third party administrators of the Plan must be provided with a copy of the changes to the Plan Amendment.

Regulation Approved: 04/23/12