DUTY TO PROTECT

All employees will safeguard Protected Information that is under the custody or control of the Association or any of its Affiliated Entities (collectively "Association" herein). Throughout employment, and at all times thereafter, each employee will not directly or indirectly disclose Protected Information to any person or entity, including friends and family, or use Protected Information except in furtherance of his or her job duties. Protected Information may only be disclosed, disseminated, or used within or outside of the Association as required or appropriate based on the employee's job. No one is permitted to remove, transfer or make copies of Protected Information for non-Association purposes.

Third party requests for information will be handled as authorized by the service area's written guidelines or directives, and in accordance with ADMIN-406, Subpoenas and Requests for Records.

At the time of termination of employment, the employee will promptly deliver (or, at the Association's request, make available for pickup) any and all Protected Information to the Association. An employee who places any Protected Information on a non-Association device or application, capable of storing electronic data, must notify his or her supervisor upon termination of employment so that arrangements can be made to have the information returned to the Association and removed from the device or application. An electronic device or application includes a mobile phone, tablet, computer, or cloud storage website or application.

Failure to safeguard Protected Information is grounds for immediate disciplinary action, including termination, in addition to possible civil and criminal legal action.

DEFINITIONS

"Protected Information" means information defined as confidential, trade secret or proprietary under this policy.

1. **"Confidential information"** generally means any information or compilation of information that is protected from public disclosure under law or not generally known or available to the public. Confidential information may be about or concern the Association, including any of its members, volunteers, clients, customers, vendors and contractual partners.

   "Personally Identifiable Information" is a form of confidential information that identifies a person's (including an employee's) full or partial name along with any of the following:
   - complete date of birth,
   - government identification number (e.g., driver's license number, social security number, or Medicaid number),

- banking or other financial information (e.g., credit card number, bank account number, bank routing codes),
- access codes or passwords that would allow access to an individual's financial record or other private information, or
- health care information, such as the physical or mental health of a person or the fact that medical services were provided to an individual.

Not only must Personally Identifiable Information be treated as confidential but it must be stored securely, accessed only by those who have a legitimate basis to know, and shredded or completely erased when up for destruction under the relevant service area's retention schedule.

2. **"Trade secret"** generally means any invention, formula, pattern, device, or compilation of information that is used by the Association and gives it a competitive advantage over those who do not know it.

3. **"Proprietary"** generally means any business or financial information that would cause competitive harm to the Association or its Affiliated Entities if disclosed. It includes business plans and strategies, marketing research, pricing or cost information, and contracts (particularly with private entities). Proprietary also refers to non-confidential copyrighted works or intellectual property offered for sale or license.

CONFIDENTIALITY AND PRIVACY REQUIREMENTS
Confidentiality and privacy require vigilance on everyone's part. Requirements for safeguarding Protected Information are contained in ADMIN-221e.

HIPAA PRIVACY
The Association's self-insured medical plan and any other employee benefit plan subject to the federal Health Insurance Portability and Accountability Act (HIPAA) will comply with the privacy protections of HIPAA. Privacy policies and procedures related to HIPAA will apply to staff who work directly with records related to the covered plans.

FERPA PRIVACY
Records that relate in any way to students or minors must be treated as confidential information because such records are likely to be protected under the Family Educational and Privacy Rights Act (FERPA). FERPA records may include, but are not limited to, health information collected by school employees or agents, incident reporting on a claim or dispute, and documentation relating to extracurricular activity. Student information protected by FERPA may include student names, pictures or images, audio recordings, school work, and any other documentation

that identifies a student. Employees who deal with student information as part of their jobs will contact the Association's privacy officer to ensure that proper safeguards and authorizations are in place for potential FERPA-protected records.

CONFIDENTIALITY AGREEMENTS
For regulatory or other business reasons, some employees may be required to sign a non-disclosure or confidentiality agreement or other written acknowledgement as a part of their job. However, even where no agreement is obtained, all current and former employees have a legal duty to maintain the confidences of the Association.

NOTIFICATION OF BREACH
If an employee knows, or has reason to believe, that Protected Information, especially Personally Identifiable Information, is not secure or that an unauthorized person may have accessed such information, the employee must notify his or her supervisor and the supervisor must notify the Association's privacy officer.

PRIVACY OFFICER
The General Counsel, or designee, serves as the Association's privacy officer, including the privacy officer for HIPAA, and is responsible for the administration of this policy and will receive and respond to inquiries concerning compliance.

This exhibit provides direction about how employees must safeguard Protected Information, particularly as it relates to Personally Identifiable Information (PII), as defined in ADMIN-221, Confidentiality and Privacy.

1. **E-mail**: Do not send PII under the Association's custody or control via normal Association email or through any personal email accounts. Similarly, do not request to receive PII from someone outside of the Association through normal email. If you have a need to send or receive PII via email, consult the Association's Information Technology (IT) service area for secure electronic transmission options (e.g., email encryption, ShareBase, etc.). Do not send PII without making sure that you are following appropriate internal procedures for your service area.
2. **Access to PII**: Access only PII that is required for you to do your job. Do not pass this information onto any other Association employee, contractor, or third party person unless your job requires it.
3. **Storage of PII**: Store PII on limited access computer network sites under User Access Management (UAM) rights where access is restricted to those with permissions or password protection (if appropriate). Do not store or place PII on widely shared network drives (i.e., O: drive). Do not store PII on USB/flash/thumb drives.
4. **Medical Information:** Medical and health information about co-workers and their families should not be communicated via email, in meetings, or in casual conversation. An employee, however, is not precluded from voluntarily self-disclosing this information or authorizing his or her supervisor, in writing, to share limited medical information with co-workers. If an individual is ill or on sick leave, management may only communicate this information to those within the Association who have a business need to know.
5. **Use of technology to protect PII:**
   a. If you view PII on your computer monitor and passers-by are able to see your monitor, use a screen protector to shield your screen from view by others. Do not walk away from your monitor when this information is on the screen without first locking or pass-coding your computer so no one will be able to access it.
   b. Keep hard copies of PII in locked drawers or another secure location provided by your supervisor. Do not leave hard copies of this information on your desk when you are not there unless you are able to secure your workspace behind a locked door. Do not take PII to the restroom, break room, or other unsecure location.
   c. PII should not remain on fax machines or copiers, but should be immediately retrieved.

   d. Use IT's approved electronic applications or portals for sharing PII (e.g., Sharebase). Do not use any non-Association servers or applications (e.g., DropBox®) to send or provide access to PII unless it is an IT-approved cloud service.

6. **Outside Vendors:** If outside vendors (including consultants or independent contractors) will have access to PII (or might have access to PII), the vendors must be contractually obligated to protect PII. Staff overseeing those contracts should inform the Association's privacy officer, in the General Counsel's office, of the PII at issue and work with the privacy officer to determine the appropriate protective language for the contracts.
7. **Destruction of PII:** PII must be properly destroyed at the end of its retention term, as set out in the applicable record retention schedule (see ADMIN-227). PII must be permanently destroyed in a way that subsequent retrieval will not be possible and that prevents anyone from reconstructing the information. Shredding services are available to employees for hard copies and IT is able to assist employees with permanent destruction of electronic records.
8. **Storage of Protected Information on unapproved servers:** Protected Information should not be stored on non-IT approved cloud servers (e.g., OneNote). Instead, such Protected Information should be stored on an appropriate networked drive.

CONFIDENTIALITY AND PRIVACY POLICY ACKNOWLEDGEMENT

The temporary worker or contractor ("Contractor") identified below has been appointed to work with the Texas Association of School Boards, Inc. or its wholly owned subsidiary, First Public, LLC (collectively "TASB" herein). Contractor hereby acknowledges receipt of TASB's Confidentiality and Privacy Policy (ADMIN-221), which applies to TASB's Confidential Information and Protected Information as defined in said policy. Contractor agrees to abide by ADMIN-221 in addition to and consistently with any confidentiality requirements set out in any written agreement between TASB and Contractor's employer or organization. Unless the context dictates otherwise, all references to "employee" or "staff" in ADMIN-221 shall be deemed to mean Contractor even though Contractor is not employed by TASB.

Contractor

Signature: _____

Name: _____

Date: _____

Submit

v.09/2020