Employee Compliance Acknowledgement Form

Use of Sensitive Information by an Employee

I, _____, as an employee of Snook ISD (the "Organization"), do hereby acknowledge that I must comply with laws that regulate the handling of personally identifying information regarding customers, employees and others. These laws include, but may not be limited to, the Fair and Accurate Transaction Act(FACTA), HIPPA, Gramm/Leach/Bliley, and, where applicable, state identity theft laws.

I understand that I must maintain the confidentiality of both personal and business non-public identifying data. I further understand that such information may only be used for the intended business purpose and any other use of said information is strictly prohibited. In the event that I do misuse or breach any personal or business non-public identifying data, I understand I can be held fully accountable both civilly and criminally, which may include, but would not necessarily be limited to, criminal charges, federal and state fines and damages incurred by customers, employees or the Organization. I have received a copy of the Sensitive Information Security Policy("Privacy Policy"). I understand and will comply with its provisions along with other rules and regulations the Organization has in place or may institute from time to time regarding the handling of Sensitive Information so as to protect the privacy of all parties involved.

Employee Signature:_____ Date:_____

SENSITIVE INFORMATION SECURITY POLICY

of

Snook Independent School District

(the "ISD")

Snook ISD desires to create a culture of security to protect Sensitive Information, as hereinafter defined in Section 4.2.

1 PURPOSE

The purpose of this SENSITIVE INFORMATION SECURITY POLICY (this "Privacy Policy") is to inform the ISD's employees, service providers, vendors and contractors of their obligation to protect the Sensitive Information created, possessed, used or maintained by the ISD in order to prevent, detect and mitigate incidents of identity theft of the Sensitive Information.

2 AUTHORITIES

In creating this Privacy Policy, the ISD has reviewed and incorporated the applicable compliance requirements of certain federal privacy laws, regulations and rules.

Guiding legal authorities for this Privacy Policy are the Fair Credit Reporting Act ("FCRA"), specifically 16 C.F.R. Part 681, Address Discrepancies Rules, and the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), specifically section 114 thereto and the FACTA Disposal Rule codified at 16 C.F.R. Part 682.

3 SCOPE

This Privacy Policy applies to employees, contractors, consultants, temporary workers, and students at the ISD, including all personnel affiliated with third parties with access to the ISD's Sensitive Information. It is the ISD's policy to have all its employees and others with access to its Sensitive Information trained to understand and follow this Privacy Policy. The Privacy Policy training will be recurring as needed to train new personnel and to train all employees and others on material changes to the Privacy Policy.

4 THE PRIVACY POLICY

4.1 PRIVACY PROTECTION OF SENSITIVE INFORMATION. IT IS THE ISD'S POLICY THAT EVERY EMPLOYEE, SERVICE PROVIDER, VENDOR, AND CONTRACTOR THAT PERFORMS WORK FOR THE ISD PROTECT THE ISD'S SENSITIVE INFORMATION (as defined in Section 4.2 heroof) FROM INAPPROPRIATE, UNNECCESARY, UNAUTHORIZED OR UNLAWFUL USE OR DISCLOSURE.

In order to so protect the ISD's Sensitive Information, it is the ISD's policy that every employee, service provider, vendor and contractor will follow the policies set forth herein and in the ISD's Identity Theft Prevention Program.

4.2 **Sensitive Information.** For purposes of this Privacy Policy, Sensitive Information shall be defined to include the following types of information, whether stored in electronic or printed format:

4.2.1 ***Sensitive Personal Information.*** Sensitive Personal Information shall mean all information that alone or in conjunction with other information identifies an individual or entity including, but not limited to:

4.2.1.1 Personally Identifiable Information, or PII (as hereinafter more fully defined in Section 4.2.4 hereof), which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual; or

4.2.1.2 PII that the ISD may possess that comes from its employees, students, vendors, contractors or others; or

4.2.1.3 Any information, whether PII or not, that is provided to the ISD with an expectation of confidentiality.

4.2.2 ***Sensitive Student Information.*** Sensitive Student Information shall include, but not be limited to:

4.2.2.1 Identifying information that is provided by a student to the ISD with an expectation of confidentiality;

4.2.2.2 Identifying information obtained by the ISD as a result of a service provided to a student; or

4.2.2.3 Information derived from any record about a student, whether in paper, electronic, or other form.

4.2.3 ***Sensitive ISD Information.*** Sensitive ISD Information shall include, but not be limited to:

4.2.3.1 The ISD proprietary information;

4.2.3.2 Any ISD document marked "Confidential," "Sensitive," "Proprietary," or any document similarly labeled.

4.2.4 ***Supporting Definitions.*** For purposes of this Privacy Policy, the following terms shall be defined as:

4.2.4.1 **"Personally Identifiable Information"** or "PII" shall mean any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual. Also referred to as Non-public Personally Identifiable Information (NPII) and/or Non-public Personal Information (NPI).

PII refers to any item, collection, or grouping of information about an individual that the ISD maintains, including, but not limited to, educational records, financial transactions, medical history, and criminal or employment history.

Examples of PII include, but are not limited to: (a) a first and last name or first initial and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name, that reveals an individual's email address; (d) a telephone number; (e) a Social Security Number; (f) credit or debit card information, including card number, expiration date, and/or data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and/or check number; (h) a driver's license, military, or state identification number; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; (j) a vehicle identifier including license plate; (j) a uniform resource locator (URL); (k) an Internet protocol address; (l) a biometric identifier (e.g., fingerprints); (m) any other unique identifying number or characteristic; and/or (n) any information that is combined with any of (a) through (m) above or any information where it is reasonably foreseeable that the information will be linked with other information to identify an individual or allow an identity to be inferred.

4.2.4.2 **"Consumer Report"** shall mean any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

(A) credit or insurance to be used primarily for personal, family, or household purposes (such as a credit report); or

(B) employment purposes (such as a criminal background check).

4.3 Sensitivity Clarification Policy. It is the ISD's policy that if an employee is uncertain of the sensitivity of a particular piece of information, he/she should treat such information as Sensitive Information until the employee or his/her supervisor/manager can contact the ISD's Information Security Officer to obtain a determination.

4.4 Protection of Sensitive Information in Hard Copy Format. It is the ISD's policy that every employee, service provider, vendor and contractor follow the policies set forth herein in regards to the access, use and control of the ISD's Sensitive Information existing in a hard-copy or print format.

4.4.1 ***Storage Locked When Not in Use.*** File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Sensitive Information will be locked when not in use.

Storage rooms containing documents with Sensitive Information and record retention areas will be locked at the end of each workday.

4.4.2 ***Security During Usage.*** Papers, documents, records, and other forms of hard data containing Sensitive Information will be secured in each office, desk or work station by keeping as many of these papers as possible locked or stored in a secure fashion when not in use. These papers will be used in a manner that protects their contents from being seen by employees, contractors and others who do not have authority to see such Sensitive Information. These papers will be used in a manner that limits the amount of time that they are unsecured (i.e. employees do not allow papers with Sensitive Information to sit out unattended or for a period longer than is necessary to have them exposed).

4.4.3 ***"Clean Desk Policy".*** Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing Sensitive Information when not in use.

Whiteboards, dry-erase boards, writing tablets, or any other writing surface in common shared work areas will be erased, removed, or secured when not in use.

4.4.4 ***Disposal of Sensitive Information.*** When discarded, all documents containing Sensitive Information will be immediately (i) shredded using a mechanical cross cut or Department of Defense (DOD) approved shredding device or (ii) placed inside a locked shred bin that is labeled "Confidential Paper Shredding and Recycling" for shredding later in the approved shredding device.

4.5 Protection of Sensitive Information in Electronic Format. It is the ISD's policy that every employee, service provider, vendor and contractor follow the policies set forth herein in regards to the access, use and control of the ISD's Sensitive Information existing in an electronic format.

4.5.1 ***Access to Electronic Sensitive Information.***

4.5.1.1 **Storage of Electronic Sensitive Information.** Unless otherwise determined by the ISD, all Sensitive Information will be encrypted or password protected when stored in an electronic format.

4.5.1.2 **Password Access.** There are no ISD-wide passwords for access to Sensitive Information. Employees with computer access to Sensitive Information shall use their own individual "strong" passwords (in accordance with the ISD's information technology system's protocols) to access such Sensitive Information. Employees are required to guard their password from use by others.

4.5.1.3 **Password Sharing Prohibited.** No employee is permitted to share or post their password for use by others. In the event an employee believes their password has been "compromised" they should immediately notify the Technology Director, detailing the reason for such belief, and confirm with the Information Security Officer that the employee has changed the compromised password.

4.5.2 ***Transmission of Electronic Sensitive Information.***

4.5.2.1 **Internal Transmission of Sensitive Information.** Internally, Sensitive Information may be transmitted using approved ISD email. Unless otherwise determined by the ISD, all Sensitive Information will be encrypted or password protected before transmission by internal email and the sender will be careful to only send the Sensitive Information to the intended recipients.

4.5.2.2 **External Transmission of Sensitive Information.** Unless otherwise determined by the ISD, any Sensitive Information sent externally will be encrypted and password protected before transmission and the sender will be careful to only send Sensitive Information to intended recipients. Additionally, a statement such as this should be included in the email:

"This message, and any attachment(s) hereto, may contain confidential and/or proprietary information, which is the property of this [name of your ISD] and is intended for the person to whom or entity to which it was originally addressed. Any use by others is strictly prohibited. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this message or its attachments is strictly prohibited, and may be unlawful. If you have received this message in error, please delete all electronic copies of this message and its attachments, if any, without disclosing the contents, destroy any hard copies that may have been created and notify the sender immediately. If your notification is by reply email, please delete the reply from your system."

4.5.2.3 **Transmission of Sensitive Financial Information.** Only designated personnel shall transmit credit card information or other sensitive financial data, and any transmissions of such information shall occur only from designated computer(s) with ISD approved secure connection(s).

4.5.3 ***Disposal of Electronic Sensitive Information.*** All electronic Sensitive Information scheduled for disposal shall be destroyed or erased so that the Sensitive Information cannot be practicably read or reconstructed. In addition, unless otherwise determined by the ISD, a wipe utility program may be used to make all computer files unrecoverable on computers scheduled for disposal.

4.6 Requests for Disclosure of Sensitive Information. It is the ISD's policy that (i) any official request for the disclosure of Sensitive Information be handled by designated personnel under the guidance of the ISD's legal counsel. Employees shall promptly direct any request for disclosure of Sensitive Information to the ISD's Information Security Officer or, if unavailable, a member of senior management.

4.7 Suspicious Activities, Information or Documents.

4.7.1 ***Suspicious Activities.*** Employees shall promptly notify the ISD's Information Security Officer or, if unavailable, a member of senior management, if the employee observes or becomes aware of any suspicious action or activity in regards to any Sensitive Information by another employee, service provider, vendor, contractor or unrelated party which could reasonably result in the inappropriate, unnecessary, unauthorized or illegal use or disclosure of Sensitive Information.

4.7.2 ***Suspicious Information or Documents.*** Employees shall promptly notify the ISD's Information Security Officer or, if unavailable, a member of senior management, if the employee is presented with, observes or becomes aware of:

(a) identification documents provided by a party or applicant conducting or attempting to conduct business with the ISD that (i) appear to have been altered or forged or (ii) are not consistent with the appearance of the party or applicant presenting the identification; or (iii) are not consistent with other information being provided by, or previously obtained from, the party or applicant; or

(b) personally identifying information provided by the party or applicant conducting or attempting to conduct business with the ISD that is not consistent with other personally identifying information provided by, or previously obtained from, the party or applicant.

5 ENFORCEMENT

Any employee found to have violated this Privacy Policy may be subject to disciplinary action, up to and including termination of employment.

6 POLICY REVIEW & UPDATE

6.1 Annual Report. It is the ISD's policy to have the ISD's Information Security Officer report, at least annually, to the ISD [Board or committee or designated member of senior management] on the effectiveness of this Privacy Policy in maintaining the protection of the ISD's Sensitive Information from inappropriate, unnecessary, unauthorized and/or illegal use and/or disclosure; including, but not limited to (i) addressing the risk of identity theft; (ii) any incidents involving identity theft; and (iii) the ISD's Information Security Officer's recommendations for changes to this Privacy Policy.

6.2 Review and Update.

6.2.1 ***Material Occurrence.*** This Privacy Policy will be reviewed and, if appropriate, updated whenever there is a material change to operations, structure, business or location, or, if applicable, when there has been (i) an incident involving the ISD's identity theft, or (ii) a suspicion of an inappropriate, unnecessary, unauthorized or illegal use or disclosure of Sensitive Information.

6.2.2 ***Annual Review.*** Notwithstanding the foregoing, this Privacy Policy will be reviewed annually, on or before [date], and, if appropriate, updated to modify the Privacy Policy for continued effectiveness and for any changes in the ISD's operations, structure, business, or location.

ADOPTION OF PRIVACY POLICY

In accordance with the governing procedures of Snook ISD, this Sensitive Information Security Policy is adopted by the ISD, effective as of the date set forth below.

Signed: R. Ray Williams

Title: Superintendent

Date: 3-21-12