STONE ACADEMY

GRAMM-LEACH-BLILEY

INFORMATION SECURITY PLAN

Background

The Gramm-Leach-Bliley Act of 2000 (GLB) mandates that financial institutions must take steps to safeguard the security and confidentiality of customer information. The Federal Trade Commisssion (FTC) ruled that GLB applies to institutions of higher education. Compliance with GLB involves compliance with (1) the **privacy** provisions of the act and (2) provisions regarding the **safeguarding** of customer information. The FTC has said that schools are deemed in compliance with the privacy provisions of GLB if they are in compliance with the Family Educational Rights and privacy Act (FERPA). With respect to the second area, GLB specfies new requirements for schools to safeguard on-public customer informtion, such as family financial information and social security and identification numbers, by having an institutional security program and security plans in specifice offices of the school that handle such information.

Designated Security Program Officers

The disignated GLB Security Program Officers for Stone Academy are Eric Jay, Chief Finance Director, and Judy Scire, Director of Compliance. All correspondence and inquires about the Stone Academy Information Security Plan should be directed to one of these Officers.

Customer Information

For purposes of FERPA and GLB, the School considers students, employees, and alumni or any other third party engaged in a financial transaction with Stone Academy as "customers." Customer information that must be safeguarded is "any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form." It includes financial information, academic and employment information, and other private paper and electronic records.

Privacy Provisions

With respect to the privacy provisions of GBL Act, Stone Academy is in compliance with FERPA. Directory inforamtion (for example, name, address, enrollment at the school and degree information) is considered public (unless a student has requested othrwise in writing). All non-difrectory information is restricted or confidential, what GLB calls "non-public." Under FERPA, restricted information (for example, academic or financial records) is released outside the school only with the student's written consent. Designated school officials, including faculty, key employees and occasionally outside service providers, have access to restricted, "non-public" informtion on a need-to-know basis only. Confidential information (for example, a faculty member's or administrator's private notes) is even more protected than restricted information and released only in certain unusual circumstances as outlined in FERPA. Although FERPA if narrowly construed only applies to enrolled students and past students, in compliance with GLB and long standing good practice, the School extends FERPA privacy protectios to all customers of the School.

The Registrar will provide guidance in complying with all FERPA privacy regulations. In addition, the School also complies with HIPAA (Health Insurance Portability and Accountability Act of 1996) with the Health Center and Human Resources providing guidance on this Act. Each department is responsible for securing customer information in accordance with all privacy guidelines.

Security Provisions

With respect to the safeguarding privision of the GLB Act, the Stone Academy GLB Information Secrity Plan herein is designed to ensure the security, integrity, and confidentiality of non-public customer information, protecting it against anticipated threats and guarding it against unauthorized access or use. Covered under the Plan are administrative, technical, and physical safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of non-public customer information. The Plan covers actions by both employees of the School and outside service providers.

The policies incorporated in this document apply to all School departments. In addition, in the case that individual departments may have additional security provisions, they will maintain written documentation of these and will make them available to the Security Program Officers. For example, the information technology department will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

The School security policy for deparmtnets include the elements described in the following sections.

Physical Safeguards

The School uses direct personal control or direct supervision to control access to and the handling of all non-public customer information when an office is open. Whether the informtion is stored in paper form or any electornically accessible format, deparmtental non-public information is maintained, stored, transmitted and otherwise handled under the direct peronal control of an authorized employee of the School.

Departmental non-public information is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning non-public information are held in private. Papers with non-public information are mailed via official campus mail, US mail, or private mail carrier. Departments are encouraged to password-portect electronic files of non-public information transmitting electronically.

When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is routinely shredded or otherwise destroyed.

Confidential material is kept secure. Most offices have locked windows and locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors; and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time.

Key access is limited to authorized School employees only in the context of School key control governing the distribution of keys.

Technical Safeguards

The School relies on the Information Technology Departent to provide network security and administrative software password access security according to industry standards in order to protect non-public custmer informtion that is accessed elecgtronically but stores outside of a department.

Departmental desktop compuers and other electronic devices storing non-public customer information are protected by physical safeguards.

Employee Management and Training

All School employees including part-time and temporary employees and volunteers are given specific training by their supervisors about issues of security of sentsitive and confidential material used in their respective offices Emplyees are held accountable to know tht although they have access to non-publc informtion in order to perform their duties for the School, they are not permitted to access it for unapproved purposes or disclose it to unauthprized persons. The Employee Handbook, which is provided to all employees, states that violation of security policies could result in termination of employment.

Outside Service Providers

Each School will assure that third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access.