Oxford Academy of Hair Design

Cyber Security Policy & Information Security Program

Overview: This Security and Cybersecurity policy & Information Security Program intends to provide direction and guidance to Oxford Academy of Hair Design on cybersecurity, risk management and protecting student information. This policy is critical to the security of the schools' operation. The cybersecurity policy utilizes best practices and standards in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The objectives of the GLBA standards for safeguarding information are to:

- Ensure the security and confidentiality of student information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student (16 C.F.R. 314.3(b)).

Purpose:

- This policy informs all Oxford Academy of Hair Design (OAHD) community members, which includes employees, students, prior students, alumni, parents, contractors, and vendors, of their responsibilities related to maintaining the privacy and security of institutional information and information technology resources.
- Protection of information and information technology resources is critical to ensuring the confidentiality, integrity, and availability of that information and to support the ongoing success of OAHD and the administrative, academic, and business units of its component institutions.
- For purposes of security, "student information" means any information about a student and/or employee, or information the institution receives about the student of another financial institution, that can be directly or indirectly attributed to the student. This Security Program, in and of itself does not create a contract between the student and any student or entity.

Responsibilities:

Chief Security Officer (CSO) – Kellie Steeves

CSO will serve as the qualified individual responsible for overseeing and implementing the Cyber security program and enforcing the Information security program. The CSO shall design, implement and maintain new safeguards as she determines to be necessary from time to time. The CSO shall report to the CIO who has the responsibility for overseeing the Program. The CSO may delegate or outsource the performance of any function under the Information Security Program as she deems necessary from time to time.

Contact information: (203) 231-8045
Kellie@oxfordhairacademy.com or oxfordhairacademy@gmail.com

Chief Information Officer (CIO) David Steeves

CIO will serve as a senior member of our personnel responsible for direction and oversight of the CSO and requires the service provider to maintain an information security program that protects the Institution with the requirements of this part.

Contact information: (203) 668-3803
Dave@oxfordhairacademy.com or steevesgc@gmail.com

Employee Access to the Security Policy: All Employees with access to student files or sensitive data on computers or software will be given our Information and Cyber Security Policy when they hired and sign off that they have read and understand the policy. They will receive an updated policy each October 1st at the same time as the Annual Crime and Safety Awareness policy and they will reply to the email acknowledging they have read it and understand. We will also post our security policy on our website https://www.oxfordhairacademy.com/disclosures Employees will also attend yearly training sessions on cyber security each October. Ensuring employees understand cybersecurity policies and their specific roles and responsibilities. We will conduct simulations and evaluate how staff will respond to a security incident. All OAHD employees have responsibility for protecting the confidentiality, availability, and integrity of OAHD and its institution's information and information technology resources.

Administrators Roles and Responsibilities:
Ensure that you have read and understand this cyber security and information security policy. Ensure that you attend yearly training courses. Ensure that your computer is accessed only by MFA. Do not share your password. Do not log on to software on any computer other than the company issued computer to access student information such as SMART or BEN. Only use Microsoft 365 email to communicate using the domain email address provided. Do not open emails or attachments from someone you do not know. Notify the SCO if you suspect or have any security event. Notify the SCO immediately if you or an Instructor notifies you of any security event. Access this security policy at any time on our website.

Instructor Roles and Responsibilities:
Ensure that you have read and understand this cyber security and information security policy. Ensure that you attend yearly training courses. Ensure that your computer is accessed only by MFA. Do not share your password. Do not log on to software on any computer other than the company issued computer to access student information such as SMART. Only use Microsoft 365 email to communicate using the domain email address provided. Do not open emails or attachments from someone you do not know. Notify the SCO if you suspect or have any security event. Notify the SCO immediately if you have a security event. Access this security policy at any time on our website.

Vendors Access:
Vendors or Guests must access the server as a "guest" SID and not the same SID as the access granted to authorized users.

Storage Locations of physical sensitive data:
Locked Filing Cabinets

Inventory of equipment:
Hardware:
10 Laptops Total
Administrators: Kellie, Brooke, Kathleen, Brittany, Ashley
Instructors: (Alexa, Sheryl, Emily, Nikki, KC)
1 IPad – Front desk – Used for checking out clients and credit card processing (no student data)
Xfinity Modem / Network

Software: (3rd Party) – All Secure Cloud Based
Gmail/Gsuite – Cloud (encrypted)
Microsoft 365 – Cloud (encrypted)
Edlumina (CRM) – Cloud (encrypted)
ONLINE SMART (SLS) (Compiled Net Code and anti SQL Injection Technology-Encrypted with SSL encryption on DELL Server
BEN (FA) – Cloud (encrypted)
Quickbooks (bookkeeping) – Cloud (encrypted)

Access to and use of institutional information protected by regulation or industry requirement, including but not limited to the following, shall follow all requirements defined in the relevant standard(s):

- FERPA – Family Educational Rights and Privacy Act
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach Bliley Act
- PCI-DSS – Payment Card Industry – Data Security Standard

Risk Assessment - Identify and Protect:
The Institution's assessment, based on the framework established by the National Institute of Standards and Technology, is a review of the school's security controls. The effectiveness of each control is determined by evaluating its policies, procedures and formal governance as well as its technical implementation. Assessment of the controls allows implementation of safeguards to control risks and provides insight into the security program. Cybersecurity risk assessments shall be performed, documented, actioned, tracked, reviewed, and revised.

The assessment also determines reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer and student information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.
The criteria used to evaluate the Institutions controls and identify the risks will be based on the school's internal systems including where data is stored, who has access, what protections are currently in place, the amount and type of electronic devices being used, as well as how they are used. Identifying the risks and threats we face in each category and updating the processes within a reasonable timeframe.

We review our data including information, files and programs to minimize the unnecessary retention of data.

Design & Implementation:
Once critical infrastructure is identified, Oxford Academy of Hair Design will protect these critical assets by:
Firewall updates on all devices: Firewalls are the first line of defense for a network ensuring it meets best practices and utilizes effective hardening techniques.

- Ensuring each employee uses multi-factor authentication (MFA) by Microsoft 365 and only authorized users will only have access to the programs and applications that are needed to complete their duties.
- Encrypting sensitive data by utilizing Microsoft 365 (secure encrypted file storage), both while stored on computers and when transmitted to other parties or stored on its system.
- Conducting regular backups of data and keeping an offline backup (Cloud) to protect against ransomware.
- Updating systems and software regularly, automating updates when possible.
- Safely disposing of electronic files and old devices. Securely delete and destroy data when no longer needed or required.
- Conducting yearly cybersecurity trainings for employees. Ensure employees understand cybersecurity policies and their specific roles and responsibilities. Conduct simulations and evaluate how staff will respond to a security incident.
- Annual ***Penetration testing***, which is a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.
- Monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, student and/or customer information by such users.

Procedures:

1. All records containing customer information shall be stored and maintained in a secure area.
2. Paper records shall be stored in the SCO's office locked in a secure filing cabinet. The owner/SCO shall control access to this area.
3. All storage areas shall be protected against destruction or potential damage from physical hazards, like fire or floods.
4. Electronic Student information shall be stored on secure servers. Access to such information shall be password controlled, and the CSO shall control access to such servers.
5. All Student information shall be backed up on a cloud [daily] basis. Such back up data shall be stored in a secure location as determined by the CSO.
6. All electronic transmissions of student and employee information, whether inbound or outbound, shall be performed on a secure basis.
7. To the extent sensitive data must be transmitted to the Institution by electronic mail, such transmissions shall be password controlled or otherwise protected from theft or unauthorized access at the discretion of the CSO
8. Require that all inbound transmissions of student information delivered to the Institution via other sources be encrypted or otherwise secured
9. The CSO shall supervise the secure disposal of all student records, documents or other sensitive data including both paper and computer hardware.

Regular Testing:

- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.
- Conduct simulations and evaluate how staff will respond to a security incident.

Improvement plan based on testing:

After regular testing and evaluating the effectiveness of the control systems ensure changes are made to any operations or areas that show risk or possible impact on the security information program. The SCO will document any changes made. Cybersecurity risk assessments shall be performed, documented, actioned, tracked, reviewed, and revised

Overseeing third party Servicers:

- The SCO ensures that all third parties have the equivalent security protections as our policy or greater by requiring encrypted cloud-based server.
- Requesting a copy of their cyber security policy and procedures.
- The CSO and third party service shall review all students' applications to ensure an appropriate level of security both within the Institution and within the Institutions business 3rd party servicer and IRS.

Incident Response Plan (IRP):

The response plan is designed to promptly respond to and recover from any security event materially affecting the confidentiality, integrity or availability of customer information.

Procedures for Responding, Notification, Escalation and Containment:

- Immediately document the breach and exactly what happened.
- Take photos if necessary, document the time and what you were doing.
- If you suspect there was a breach or other security incident immediately notify the CSO (Kellie Steeves) by phone 203-231-8045 or email Kellie@oxfordhairacademy.com or oxfordhairacademy@gmail.com
- The SCO will report the breach to FSA by emailing CPSSAIG@ed.gov or by filling out the Cybersecurity Breach Intake Form.
- Document the breach including employees, times, dates.
- Evaluate and revise the IRP following a security event.

The SCO will report in writing annually to the SIO and include the following information:

(1) The overall status of the information security program and your compliance with this part; and
(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.