



Gramm–Leach–Bliley (GLB) Act & Fair and Accurate Credit Transactions (FACT) Act Information Security and Identity Theft Prevention Plan

Purpose and Background

The Art Academy of Cincinnati (AAC) establishes this Plan to protect confidential records and address identity theft risks. The Plan applies to AAC personnel and service providers that handle covered information and is supported by internal procedures and security records.

The Gramm–Leach–Bliley Act of 1999 (GLBA) and its Safeguards Rule, 16 CFR Part 314, govern protection of covered customer information. AAC’s participation in federal student aid programs requires compliance with the Safeguards Rule. The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) amended the Fair Credit Reporting Act and provides for identity theft prevention and secure disposal of consumer report information.

GLBA and FACT Act Requirements

AAC shall designate a Qualified Individual, assess risks, implement appropriate safeguards, monitor their effectiveness, train personnel, oversee service providers, and periodically adjust its information security program. The safeguards shall be appropriate to AAC’s size, activities, and the sensitivity of the information handled.

The FACT Act Red Flags Rule, 16 CFR 681.1, applies to covered financial institutions and creditors offering or maintaining covered accounts. Its definitions differ from those used under GLBA. AAC shall document its applicability assessment and use Appendix A for identity theft prevention. GLBA coverage alone does not establish Red Flags Rule coverage.

Designated Security Program Officials

Qualified Individual: **Kyle Grizzell, Technical Alignment Manager, Keystone Solutions.**

Senior AAC Official Responsible for Oversight: **Joe Girandola, President and CEO.**

Program inquiries: **helpdesk@artacademy.edu.**

The Qualified Individual shall oversee implementation and enforcement of this Plan. AAC retains institutional responsibility and the President and CEO directs and oversees the external arrangement. Keystone Solutions shall maintain an information security program protecting AAC as required by the Safeguards Rule.

Customer Information and Privacy

GLBA-covered information includes nonpublic personal information obtained in providing financial services to current or former students, including financial aid administration. Examples include student financial records, tax and income information, Social Security numbers, and banking or loan information, in paper or electronic form.

AAC also requires appropriate protection of other confidential student, employee, alumni, and institutional records under applicable policies and laws. This broader institutional protection does not redefine those records as GLBA-covered information.

Education records shall be disclosed in accordance with FERPA, including consent requirements and lawful exceptions. Directory information may be disclosed only in accordance with AAC's published FERPA notice and applicable restrictions. The office responsible for student records shall provide FERPA guidance.

Security Provisions and Risk Assessment

Each department shall protect covered information throughout its collection, processing, storage, transmission, use, and disposal. Department procedures shall be available to the Qualified Individual. Access shall be limited to authorized institutional purposes.

The Qualified Individual shall maintain an inventory of information, systems, devices, facilities, users, and providers and assess foreseeable internal and external risks. AAC shall document risk evaluation, existing controls, mitigation or acceptance decisions, responsible persons, and completion dates. Assessments shall be repeated periodically and after material changes.

Physical Safeguards

Paper records shall be secured in restricted offices or locked storage. Keys and access credentials shall be limited to authorized persons. Confidential discussions, documents, and screens shall be protected from unauthorized observation. Personnel shall lock screens and secure work areas when unattended.

Off-campus work and record transportation shall use approved protections. Confidential information shall not be left in unsecured vehicles, shared spaces, or unapproved storage locations.

Technical Safeguards

AAC's IT function and providers shall implement and document the following controls:

- Individual accounts, role-based permissions, periodic access reviews, and prompt adjustment or removal of access when responsibilities or employment change.
- Multifactor authentication for covered information systems, unless the Qualified Individual approves in writing reasonably equivalent or stronger access controls.
- Encryption of covered information at rest and in transit over external networks; effective compensating controls reviewed and approved by the Qualified Individual where encryption is infeasible.
- Security evaluation of internal and external applications, controlled system changes, updates, endpoint protection, network controls, and detection and logging of unauthorized activity.
- Approved storage and transfer methods, protected backups, and recovery procedures. Credentials shall not be shared or transmitted through insecure channels.

Monitoring and Testing

AAC shall regularly monitor or test safeguards and track remediation. Unless a documented exception under 16 CFR 314.6 applies, information systems shall use effective continuous monitoring or the testing required by 16 CFR 314.4(d)(2), including annual penetration testing and vulnerability assessments at least every six months and following relevant changes or circumstances.

Retention and Secure Disposal

AAC shall periodically review retention and securely dispose of covered customer information no later than two years after its last use to provide a product or service, unless a regulatory exception applies, including legitimate business need, legal retention obligations, or infeasibility of targeted disposal. Applicable student aid retention requirements and legal holds shall be preserved.

For consumer report information maintained for a business purpose, AAC shall use reasonable disposal measures under 16 CFR Part 682. Paper shall be shredded or otherwise destroyed and

electronic information erased or destroyed so it cannot practicably be read or reconstructed. Disposal contractors shall undergo appropriate due diligence and contractual oversight.

Employee Management and Training

Employees, temporary personnel, and other authorized users shall receive security instruction appropriate to their access and duties, with updates reflecting changing risks. Training shall address phishing, fraudulent requests, record handling, identity verification, credentials, and incident reporting. AAC shall retain training records and provide relevant updates to security personnel.

Personnel shall not access records out of curiosity, use information for personal benefit, or disclose it without authorization. HR and department leaders shall notify IT promptly of changes requiring access modification. Violations shall be addressed under applicable AAC procedures.

Outside Service Providers

AAC shall evaluate providers before engagement and periodically thereafter according to their access and risk. Contracts shall require safeguards appropriate to covered information. Reviews shall identify information handled, permitted purposes, security responsibilities, subcontractor protections, incident notification, and return or destruction requirements.

Campus Cafe, Keystone Solutions, and other relevant providers shall supply security documentation needed for review. AAC shall verify controls it must configure or perform. Independent assurance reports and security assessments may support review; they do not replace AAC's own program. Confidentiality obligations, review rights, and remedies shall be addressed in the applicable contract.

Security Incident Response

Suspected loss, unauthorized access, disclosure, or identity theft shall be reported promptly to: helpdesk@artacademy.edu and to

Rick Wolhoy, Executive Director of Facilities, at rick.wolhoy@artacademy.edu.

Rick Wolhoy remains the designated incident and after-hours contact and shall promptly escalate technical incidents to the Qualified Individual and institutional oversight official.

The Qualified Individual shall coordinate containment, evidence preservation, investigation, recovery, and corrective action. Internal response procedures shall identify decision makers, communication responsibilities, verified after-hours escalation methods, and reporting duties. Email shall not be assumed to provide immediate after-hours response.

AAC shall report incidents as required by federal, state, and contractual obligations. Federal Student Aid guidance requires breach reporting within 24 hours after an incident is known or identified. FTC notification events involving unauthorized acquisition of at least 500 consumers' unencrypted information must be reported as soon as possible and within 30 days of discovery; encryption-key compromise and the rule's acquisition presumption must also be considered.

Reassessment and Institutional Oversight

AAC shall review this Plan at least annually and following material operational changes, testing findings, or incidents. Reviews shall address risk assessment, control decisions, vendors, training, incidents, and unresolved actions. The Qualified Individual shall provide a written report to the Executive leadership at least annually where 16 CFR 314.4(i) applies. AAC retains annual review as an institutional practice when an exception applies.

Small Institution Exception

Any reliance on 16 CFR 314.6 shall be supported by a documented count of consumers whose covered information is maintained by or for AAC, including former students. Enrollment alone is insufficient.

The exception for fewer than 5,000 consumers covers only 314.4(b)(1), (d)(2), (h), and (i); core safeguards and applicable notification duties remain. Written risk documentation and response procedures remain AAC practices.

Appendix A Identity Theft Prevention

This appendix establishes AAC's identity theft procedures and, where legally applicable and appropriately approved, its Red Flags Program. Finance, Financial Aid, Student Accounts, IT, and the designated officials shall coordinate implementation.

Applicability and Covered Accounts

AAC shall evaluate whether its activities meet the Red Flags Rule's financial institution or creditor definitions and periodically assess covered accounts if subject to the rule. Relevant creditor activities include regular use of consumer reports or reporting to credit agencies in credit transactions, or advancing repayable funds, subject to statutory limitations. Billing later, accepting credit cards, or using employment screening reports alone does not establish coverage.

Covered accounts include qualifying personal, family, or household accounts permitting multiple payments or transactions and other accounts presenting reasonably foreseeable identity theft risk. AAC shall assess tuition payment arrangements and any institutional loan accounts it actually offers; no specific loan program is presumed to exist. The documented assessment shall address account opening, access methods, and prior incidents.

Identification and Detection of Red Flags

Identity theft is fraud or attempted fraud using another person's identifying information without authority. Personnel shall identify warning signs relevant to AAC's accounts and operations, including:

- Fraud alerts or relevant warnings from reporting agencies, providers, or affected individuals.
- Altered identification, inconsistent identifying information, or failed identity verification.
- Unusual account access or changes to contact or refund information followed by unexpected transactions.
- Reports of unauthorized activity from students, account holders, law enforcement, or other reliable sources.

Authorized personnel shall verify identity when opening or accessing accounts and independently authenticate sensitive changes using established contact information. Suspected fraudulent requests shall be escalated before processing. Where AAC uses consumer reports, notices of address discrepancy shall be addressed under applicable FCRA requirements.

Response and Program Administration

Responses shall reflect the circumstances and may include contacting the account holder through a verified channel, securing access, pausing a suspicious transaction, correcting records, notifying providers or authorities when appropriate, and documenting the investigation. Responses must respect applicable student aid and refund deadlines. Procedures shall be updated as threats or operations change.

If the Red Flags Rule applies, the initial written Program must be approved by the Board of Trustees or an appropriate Board committee. A designated senior official shall oversee implementation, staff training, and provider arrangements. The GLBA small-institution exception does not determine Red Flags Rule coverage.

Policy Dates and Revision

Original policy approval: **Joe Girandola, President and CEO, April 2025.**

Original effective date: **May 15, 2025.**

This revision/review prepared: **May 3, 2026.**

Next scheduled review: **May 1, 2027;** earlier if circumstances require.

The original dates identify the prior policy. New provisions take effect upon actual approval of this revision and do not establish prior implementation.

Authorities

GLBA Safeguards Rule — 16 CFR Part 314

Identity Theft Red Flags Rule — 16 CFR 681.1

Consumer Report Disposal Rule — 16 CFR Part 682