SCHOOL OF VISUAL ARTS

# Personal Wearable Technology & AI-Enabled Devices

Effective Date: August 1, 2026

Version: 2026.09.17

Category: Data Privacy & Compliance

Applies to: All employees, faculty, staff, contractors, consultants, temporary workers, interns, volunteers, vendors, and other individuals performing services for or on behalf of SVA

Department Owner: Human Resources/Data Privacy Office

## 1. Purpose

This policy establishes guidelines regarding the use of AI enabled wearable technology, including AI glasses, smart glasses, and similar devices with recording, audio-capture, or data-transmission capabilities, in the workplace. Its purpose is to protect the privacy of students, employees, and visitors; safeguard confidential institutional information; and support compliance with the Family Educational Rights and Privacy Act (FERPA) and other applicable requirements.

## 2. Scope

This policy applies to all employees, faculty, staff, contractors, consultants, temporary workers, interns, volunteers, vendors, student workers and other individuals performing services for or on behalf of SVA. It applies at all SVA locations; during any SVA sponsored, SVA related, or work-related activity; while performing services for SVA; and whenever an individual has access to nonpublic SVA information, student information, or confidential discussions, regardless of work hours or physical location.

Visitors must comply with applicable campus rules and instructions concerning recording-capable wearable devices.

## 3. Policy

As used in this policy, “Covered Devices” means AI-enabled glasses, smart glasses, and other personal wearable technology or AI-enabled wearable devices with recording, audio-capture, biometric-capture, location-tracking, or data-transmission capabilities that are subject to this policy.

As used in this policy, “Medical Information” means information regarding an individual’s medical condition or history, including a disability, a pregnancy-related condition, or genetic information (such as family medical history or a predisposing genetic characteristic), that is obtained through a Covered Device and that indicates or could reasonably reveal such a condition, disability, or genetic information, such as heart rate, blood pressure, temperature, fatigue level, gait, electroencephalogram (EEG) data, or other vital-sign or diagnostic information, consistent with the Americans with Disabilities Act, the Genetic Information Nondiscrimination Act, the Pregnant Workers Fairness Act, applicable New York State and New York City human rights laws, and their implementing regulations. Medical Information does not include general wellness or fitness metrics, such as step counts or calories burned, that do not indicate or reveal a medical condition, disability, pregnancy-related condition, or genetic information.

Individuals covered by this policy are prohibited from wearing or using AI-enabled glasses, smart glasses, or similar wearable devices capable of recording audio, video, or capturing biometric or environmental data while performing job duties; participating in meetings; in classrooms; or in settings involving interactions with students, colleagues, or the public, regardless of the individual's physical location.

Covered Devices may not be activated, used, or configured to capture, record, livestream, transmit, analyze, store, or process audio, video, images, biometric information, location information, or environmental data in any setting covered by this policy. Where a device cannot reliably disable these functions, it may not be worn in covered settings. This policy does not apply to hearing aids, cochlear implants, insulin pumps, or other assistive or medical devices that are not designed or primarily used to record, transmit, or capture audio, video, images, or biometric or environmental data of others.

This includes devices that:

ÏRecord video or audio;

ÏCapture images;

ÏTransmit data to external servers or AI processing systems;

ÏUse facial recognition or biometric identification features; or

ÏCapture, analyze, store, or process location information or environmental data.

Individuals may not upload, transmit, sync, or submit recordings, images, transcripts, biometric data, or other information obtained in connection with SVA work to personal cloud-storage accounts, consumer artificial-intelligence tools, social-media platforms, or other third-party services unless expressly authorized by SVA and consistent with applicable privacy, information-security, contractual, and records-retention requirements.

Where an approved use permits a Covered Device to transmit data to an AI processing system, that data may only be transmitted to and processed using an SVA-provided or SVA-approved AI platform operated under an active institutional license, consistent with SVA's data classification requirements. Confidential institutional or student information may not be uploaded to or analyzed in any AI platform, including through an AI-enabled wearable device, without prior review by the Data Privacy Office.

Recording-capable wearable devices may not be used in restrooms, lactation rooms, health or counseling spaces, or other areas where individuals reasonably expect privacy. They also may not be used during meetings or interactions involving student records, personnel matters, health information, disciplinary matters, accommodations, legal advice, or other confidential information unless expressly authorized.

Where the collection of biometric identifier information through a Covered Device is permitted under an approved exception in Section 4, any collection, capture, conversion, storage, or sharing of biometric identifier information (including facial geometry, retina or iris scans, fingerprints, or voiceprints) through a Covered Device requires advance approval from the Data Privacy Office and, where applicable, prior notice to or consent from the individuals whose biometric identifier information is collected, except that this advance-approval and notice/consent requirement will not be applied in a manner that denies or unreasonably delays a legally required reasonable accommodation for a qualified individual with a disability. Where an approved disability accommodation involves the collection of biometric identifier information through a Covered Device, the Data Privacy Office will coordinate with Human Resources, as applicable, so that any necessary approval and notice is addressed as part of, and concurrently with, the accommodation review

described in Section 4, consistent with the interactive process and timeliness obligations of the Americans with Disabilities Act. Consistent with New York Labor Law, no individual will be required, as a condition of obtaining or continuing employment, to be fingerprinted or to otherwise provide biometric identifier information except as permitted by law. SVA will not sell, lease, trade, or otherwise profit from biometric identifier information collected through a Covered Device.

## 4. Exceptions and Required Accommodations

This policy will be administered consistent with applicable federal, New York State, and New York City law.

Reasonable accommodations. An employee may request an exception or alternative to this policy as a reasonable accommodation for a disability, pregnancy, childbirth or a related medical condition, or sincerely held religious belief or practice. Requests will be reviewed through the applicable Human Resources accommodation process and, where appropriate, through an interactive or cooperative dialogue. Any accommodation will be considered on an individualized basis and may be granted unless it would create an undue hardship or a direct threat that cannot be reduced through reasonable measures. Where an approved accommodation involves the collection of biometric identifier information through a Covered Device, Human Resources, as applicable, will coordinate with the Data Privacy Office so that any approval required under Section 3 is obtained as part of, and does not unreasonably delay, the interactive or cooperative dialogue and the accommodation determination.

Nondiscriminatory use of device-generated data. Any Medical Information inadvertently captured by a Covered Device will be treated as confidential medical information, maintained separately from personnel files with limited access, and will not be used as a basis for an employment decision affecting an employee's race, color, religion, sex (including pregnancy, childbirth, or related medical conditions), national origin, age, disability, or genetic information, consistent with the Americans with Disabilities Act, Title VII, the Pregnant Workers Fairness Act, and other applicable equal-employment-opportunity laws.

Approved institutional use. SVA may authorize the use of a recording-capable wearable device for a defined institutional purpose, including approved accessibility, safety, instructional, or operational needs. Any approved use must comply with applicable privacy, data-security, recording-consent, and student-record requirements, including FERPA where applicable. Approval must be obtained in advance from Human Resources and the Data Privacy Office. Any institutional use that directs

an individual to wear a device collecting physiological, health-related, or other Medical Information must be voluntary, unless the use is job-related and consistent with business necessity, consistent with the Americans with Disabilities Act's limitations on disability-related inquiries and medical examinations.

Participant consent. Before using an approved recording-capable wearable device to record, transcribe, or summarize a conversation or gathering, the authorized user must obtain the affirmative permission of all participants. If a participant declines or withdraws permission, the device must be deactivated for that conversation or gathering. This requirement does not apply to the extent it would deny or unreasonably delay a legally required reasonable accommodation for a qualified individual with a disability, and the accommodation will not be conditioned on other participants' affirmative permission; however, SVA will provide notice to other participants consistent with applicable law, and any resulting recording or data capture must be limited to use for the accommodated individual's own individual work purposes, may not be reproduced, distributed, or shared with any other person or platform, and must be destroyed or securely deleted at the end of the course or activity unless a longer period is required by law or Section 4's written-approval and data-safeguard requirements. This exception does not authorize, and does not modify, the prohibition elsewhere in this policy on recording a collective-bargaining or grievance session.

Written approval and data safeguards. Any approval under this policy must be documented in writing and identify the specific device, authorized user, permitted purpose, location or activity, duration, permitted data collection, data-storage location, and required safeguards. Recordings or data collected through an approved exception must be limited to the approved purpose, retained only for the period required by the applicable institutional records-retention schedule or legal requirement, protected by appropriate access controls, and securely deleted or disposed of when no longer required. Approval may be modified or revoked if the authorized use changes or creates a privacy, security, or legal concern.

Student education records (FERPA). A recording or other data capture obtained through a Covered Device that is directly related to an identifiable student and is maintained by SVA may constitute an "education record" under FERPA. Any such record will be maintained, accessed, and disclosed consistent with FERPA, including obtaining the prior written consent of the parent or eligible student before disclosure outside a FERPA exception, affording the parent or eligible student the opportunity to inspect and review the record, and redacting or segregating information directly related to other students where this can be done without destroying the meaning of the record.

Vendor agreements and data use. Any agreement for the purchase, lease, or licensing of an AI-enabled wearable device or related AI processing service must be reviewed and approved through SVA's information-technology and contracting processes and must include terms governing the privacy and security of SVA data and limiting the vendor's ability to use SVA data to train, develop, or improve the vendor's AI models. Ownership and permitted use of any transcript, recording, or other content generated through an approved use of a Covered Device is governed by SVA's intellectual property policies and any applicable license terms, and users should be aware that the copyright status of AI-generated content remains unsettled under current law.

Legal and protected activity. Nothing in this policy is intended to restrict activity protected by applicable law, including employees' rights to engage in protected concerted activity under the National Labor Relations Act, where applicable, or to make reports, participate in investigations, or exercise other rights protected by law. Consistent with National Labor Relations Board guidance, a Covered Device may never be used to surreptitiously record a collective-bargaining or grievance session, and any proposed use of surveillance or recording technology affecting the working conditions of a bargaining-unit employee remains subject to any applicable collective-bargaining obligations.

Emergency situations. This policy does not prevent the use of a device to contact emergency services or to respond to an immediate threat to health or safety. Any recording or data capture in an emergency must be limited to what is reasonably necessary under the circumstances and handled in accordance with applicable law and institutional procedures.

No automatic recording exception. An approved accommodation or institutional use does not authorize recording, transmission, facial recognition, biometric identification, or other data collection beyond the scope specifically approved. Any such activity must comply with applicable law and institutional requirements.

## 5. Reporting of Privacy or Security Incidents

Any individual who becomes aware of an actual or suspected unauthorized recording, transmission, access, loss, or disclosure involving a Covered Device must promptly report it to Human Resources and the Data Privacy Office. SVA will assess the incident and take appropriate responsive measures consistent with applicable law and institutional procedures.

## 6. Enforcement

Violations of this policy may result in corrective action, up to and including termination of employment or termination of a vendor relationship, consistent with applicable law, collective bargaining obligations, and SVA policy.

## 7. Personal Devices; No Institutional Liability

Covered Devices used under this policy remain the personal property and responsibility of the individual who owns or operates them. SVA assumes no responsibility for the loss, damage, malfunction, or unauthorized use of a personal Covered Device and does not undertake any duty to monitor use of personal wearable technology beyond the terms of this policy. An individual who violates this policy or uses a Covered Device to make an unauthorized recording of another person does so at their own risk and may be individually responsible for any resulting harm, including under applicable wiretapping, eavesdropping, or other privacy laws

## 8. Policy Administration and Review

The Data Privacy Office, in consultation with Human Resources and Information Technology, is responsible for reviewing this policy periodically and updating it as necessary to reflect changes in technology, law, or institutional practice. Individuals with questions about a use of AI-enabled wearable technology that this policy does not clearly address should contact the Data Privacy Office for guidance before proceeding.