ChiME
Chicago Center
for Music Education

True potential through the power of music

Student Data Privacy Policy
Chicago Center for Music Education

The Chicago Center for Music Education (legal name “Suzuki-Orff School for Young Musicians,” a.k.a “ChiME”) is committed to protecting the privacy, confidentiality, and security of information relating to students who participate in ChiME programs, including students served through Chicago Public Schools ("CPS") and other educational partners. ChiME recognizes that student information is entrusted to the organization for the limited purpose of providing high-quality music education and related educational services. ChiME will collect, access, use, disclose, retain, and dispose of student information only as necessary to provide those services and in accordance with applicable federal, state, and local laws, contractual requirements, and the policies of its educational partners. This Policy is intended to support ChiME's compliance with applicable requirements, including the Family Educational Rights and Privacy Act ("FERPA"), the Illinois Student Online Personal Protection Act ("SOPPA"), the Illinois School Student Records Act ("ISSRA"), applicable CPS policies and contractual requirements, and other applicable privacy and information-security laws. Where a CPS contract, data privacy agreement, or applicable law imposes requirements that are more restrictive than this Policy, ChiME will follow the more restrictive requirement.

ChiME will treat information received from CPS or another educational partner as confidential regardless of whether the information is maintained electronically or in paper form.

This Policy applies to:

- All ChiME employees, instructors, teaching artists, contractors, volunteers, interns, and other individuals who have access to student information.
- Student information received from CPS or another educational partner.
- Student information collected directly by ChiME in connection with its educational programs.
- Student information created or maintained by ChiME in connection with providing educational services.
- Paper and electronic records, databases, spreadsheets, email, photographs, audio recordings, video recordings, and other media containing student information.

Security Safeguards

ChiME will implement reasonable administrative, technical, and physical safeguards appropriate to the nature and sensitivity of Student Information.

Safeguards may include:

- Password protection and access controls;
- Limiting access based on job responsibilities;
- Use of secure, reputable systems for storing electronic information;
- Encryption or other appropriate protections when transmitting or storing sensitive information;
- Secure disposal of paper records;
- Secure deletion of electronic records when they are no longer required;
- Protection of devices used to access Student Information;
- Reasonable measures to prevent unauthorized copying or downloading;
- Regular review of user access;
- Training of personnel regarding confidentiality and data security; and
- Procedures for responding to suspected or confirmed security incidents.

ChiME will take reasonable measures to protect Student Information from unauthorized access, destruction, use, modification, or disclosure.

Access Controls

ChiME will provide access to Student Information only to personnel who require such access to perform their assigned duties.

Personnel with access to Student Information must:

- Keep login credentials confidential;
- Not share accounts or passwords;
- Not leave Student Information accessible to unauthorized individuals;
- Not download or copy Student Information unless necessary for their responsibilities;
- Not store Student Information on personal devices or personal accounts unless expressly authorized and appropriately protected; and
- Immediately report suspected unauthorized access, loss, disclosure, or other security incident.

Access will be removed or modified when an employee, contractor, volunteer, or other authorized user no longer requires access.

Use of Photographs, Audio, and Video

Photographs, audio recordings, and video recordings of students may constitute Student Information. ChiME will use student photographs, recordings, or other student media only for purposes authorized by the applicable school, CPS agreement, parent/guardian consent or release where required, and applicable law. ChiME will not publicly identify a student in connection with a photograph, recording, performance, or other media unless the applicable authorization permits such identification. ChiME will not use student photographs, recordings, or other media for unrelated commercial advertising without appropriate authorization and signed media release on file.

Personnel Confidentiality and Training

Employees, teaching artists, contractors, volunteers, and other individuals with access to Student Information will receive appropriate instruction regarding confidentiality, privacy, and security requirements.Personnel are expected to understand that their obligation to protect Student Information continues after their employment, contract, volunteer service, or other relationship with ChiME ends. ChiME may require individuals with access to Student Information to sign confidentiality agreements or acknowledgments when appropriate.