Whole Life Farm Arts & Music Foundation

SECTION 13 - PRIVACY & CONFIDENTIALITY POLICY

Policy & Governance Handbook

Draft for Board Review and Adoption

Purpose: This policy establishes standards for protecting personal, organizational, donor, participant, youth, financial, and other confidential information received or maintained by the Foundation in connection with its charitable programs and operations.

1. POLICY STATEMENT

The Foundation respects the privacy of participants, families, donors, volunteers, directors, employees, contractors, artists, applicants, and community members. Confidential information shall be collected, accessed, used, stored, shared, and disposed of only for legitimate Foundation purposes and with reasonable safeguards.

2. SCOPE

This policy applies to directors, officers, employees, contractors, teaching artists, volunteers, committee members, and other persons who receive access to confidential Foundation information through their role.

3. CONFIDENTIAL INFORMATION

Confidential information may include nonpublic personal contact information; information concerning minors; registration and enrollment records; emergency contacts; health, disability, allergy, or accommodation information; background-check information; donor records; nonpublic financial information; banking and payment information; passwords; personnel information; Board executive-session information; legal communications; grant information; incident reports; investigations; and other information reasonably understood to be private or sensitive.

4. MINIMUM NECESSARY ACCESS

Access to confidential information should be limited to persons who reasonably need the information to perform authorized Foundation responsibilities. Access does not authorize personal use, unnecessary copying, or disclosure to others.

5. INFORMATION CONCERNING MINORS

Information concerning children and teens shall receive particular care. Youth registration, emergency contacts, health or accommodation information, attendance, incident records, photographs, and parent/guardian communications should be accessible only to persons with a legitimate program, safety, administrative, or legal need.

6. DONOR PRIVACY

Donor names, contact information, giving history, payment information, and donor communications shall be handled with appropriate care. The Foundation shall not sell donor contact lists. Requests for anonymity should be honored to the extent practical and lawful. Public sponsor or donor recognition may occur when authorized or reasonably expected as part of the contribution or sponsorship arrangement.

7. FINANCIAL AND PAYMENT INFORMATION

Banking credentials, payment-card information, tax records, account numbers, financial reports, and other sensitive financial information shall be protected from unauthorized access. Payment information should not be retained longer or in greater detail than reasonably necessary for legitimate operations and legal compliance.

8. BOARD CONFIDENTIALITY

Directors may receive confidential information concerning personnel, contracts, legal matters, donors, investigations, finances, negotiations, or participants. Directors shall not disclose confidential Board information outside authorized channels or use it for personal advantage.

9. PERSONNEL AND CONTRACTOR INFORMATION

Employment, compensation, tax, performance, disciplinary, background-screening, and other personnel information shall be shared only with persons who have a legitimate need for access or when disclosure is legally required.

10. PASSWORDS AND DIGITAL SECURITY

Passwords, account credentials, access codes, and security information shall be protected and shared only with authorized users. Individuals should use reasonable password and device-security practices. Access should be removed when a person no longer requires it for Foundation duties.

11. EMAIL, CLOUD STORAGE, AND DEVICES

Foundation records stored in email, cloud services, computers, phones, or other electronic systems remain subject to this policy. Important Foundation records should be maintained in authorized locations rather than solely in personal accounts or devices when loss of access could materially affect the Foundation.

12. PHOTOGRAPHS, VIDEO, AND RECORDINGS

Photographs, video, audio, names, testimonials, and other identifying information may be used for Foundation communications when appropriate permission has been obtained or another lawful basis applies. Special care shall be used for minors, consistent with the Youth Protection & Child Safety Policy.

13. WEBSITE AND ONLINE FORMS

Information collected through the Foundation’s website, registration forms, donation forms, email lists, or online platforms should be limited to information reasonably needed for the stated purpose. Third-party platforms should be selected and used with reasonable attention to privacy and security.

14. SHARING WITH SERVICE PROVIDERS

The Foundation may share information with authorized service providers such as payment processors, accountants, payroll providers, background-check providers, insurers, registration systems, grant administrators, or technology vendors when reasonably necessary. Only information appropriate to the service should be shared.

15. LEGALLY REQUIRED DISCLOSURE

Confidential information may be disclosed when required by law, subpoena, court order, mandatory reporting obligations, government inquiry, insurance requirements, or when reasonably necessary to protect a person from serious harm. When appropriate, the Foundation may seek legal advice before disclosure.

16. SAFETY AND MANDATORY REPORTING

Confidentiality shall not be used to prevent legally required reports of suspected child abuse or neglect, threats to safety, or other matters that must be reported. Youth-safety reporting shall follow the Youth Protection & Child Safety Policy and applicable law.

17. INCIDENTS AND INVESTIGATIONS

Information concerning complaints, whistleblower reports, harassment allegations, safety incidents, or investigations shall be shared only as reasonably necessary to review the matter, protect participants, take corrective action, obtain professional advice, or comply with law. Absolute confidentiality cannot be promised.

18. RECORD RETENTION AND DESTRUCTION

Confidential records shall be retained and destroyed in accordance with the Record Retention & Document Destruction Policy. When destruction is permitted, sensitive paper and electronic information should be disposed of using reasonable methods that reduce the risk of unauthorized recovery.

19. LOST OR IMPROPERLY DISCLOSED INFORMATION

Suspected loss, theft, unauthorized access, mistaken disclosure, compromised passwords, or other privacy or security incidents should be promptly reported to an appropriate Foundation leader. The Foundation shall assess the incident and take reasonable corrective steps, including professional or legal consultation when appropriate.

20. CONFIDENTIALITY AFTER SERVICE

The obligation to protect confidential information continues after a director, officer, employee, contractor, or volunteer leaves the Foundation to the extent the information remains confidential and applicable law permits.

21. PERSONAL INFORMATION REQUESTS

The Foundation should respond reasonably to requests to correct or update personal information it maintains when appropriate. Certain records may need to be retained despite a request for deletion because of legal, financial, grant, safety, insurance, or recordkeeping obligations.

22. NO PERSONAL USE

Confidential Foundation information shall not be used for personal marketing, private business solicitation, personal disputes, political campaigning, harassment, identity theft, or other purposes unrelated to authorized Foundation activities.

23. VIOLATIONS

A violation of this policy may result in removal of access, reassignment, discipline, termination of employment or contract, removal from volunteer duties, Board action, or other corrective measures appropriate to the circumstances.

24. POLICY REVIEW

The Board should periodically review this policy, particularly as the Foundation adopts new registration systems, payment platforms, donor databases, youth-program systems, employee systems, or other technologies involving personal information.

25. ADOPTION

This Privacy & Confidentiality Policy becomes effective when approved by the Board of Directors and remains in effect until amended or replaced by the Board.

CONFIDENTIALITY ACKNOWLEDGMENT

Individuals with regular access to confidential information may be asked to sign this acknowledgment.

Name:	_____
Role:	_____
Acknowledgment:	I received, reviewed, and agree to follow the Privacy & Confidentiality Policy.
Signature:	_____ Date: _____

BOARD ADOPTION RECORD

Date adopted:	_____
President:	_____
Secretary:	_____
Board vote:	_____ in favor _____ opposed _____ abstained

Document status: DRAFT - not effective until formally adopted by the Board of Directors.