Data Retention Policy

This policy is to be reviewed biennially. Last reviewed 23/10/25

For the purposes of this document, Wiltshire Young Musicians (WYM) includes WYMT Ltd and the Committee members acting on behalf of the trustee.

Wiltshire Young Musicians is hereinafter referred to as "the charity."

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the charity's guidelines on retention are consistently applied throughout the organisation.

2.0 Purpose

The purpose of this policy is to specify the charity's guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all charity data stored on charity-owned, charity-leased, and otherwise charity-provided systems and media, regardless of location. Note that the need to retain certain information will comply with EU General Data Protection Regulation GDPR and the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

4.0 Policy

4.1 Reasons for Data Retention

The charity does not wish to simply adopt a "save everything" approach. That is not practical or cost effective and would place an excessive burden on charity and IT Staff to manage the constantly-growing amount of data. Some data, however, must be retained in order to protect

the charity's interests, preserve evidence and generally conform to good business practices.

Some reasons for data retention include:

- Safeguarding of members
- Contact with members family
- enhancement of education
- for industry related progression for agencies, auditions and other directly linked activities

4.2 Data Duplication

As data storage increases in size and decreases in cost, charities often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server and again on a backup system. When identifying and classifying the charity's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information. An information asset register will be held centrally to keep track of any data duplication.

4.3 Retention Requirements

This section sets guidelines for retaining the different types of charity data.

- Personal member data: Personal data will be held for as long as the individual is a member of the charity plus a period of 2 years.
- Personal employee and Tutor data: General employee data will be held for the duration of employment and then for a maximum of 1 year after the last day of contractual employment. Employee contracts will be held for 3 years after last day of contractual employment in case of a legal dispute occurring between the employee and the charity.
- Tax payments will be held for seven years.

- Records of leave will be held for three years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 year after interview. This personal data will then be destroyed, unless otherwise arranged with the interviewee.
- Health and Safety: Details of major accidents and dangerous occurrences. Will be held for 7 years.
- Critical data including Tax and VAT: Critical data must be retained for 7 years.
- In order that no copyright dispute can arise, any musical arrangements created by WYM ensemble tutors should be returned to the tutor or destroyed on the date at which the tutor leaves the organisation.

4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the charity will use data efficiently thereby making data management and data retrieval more cost effective. When the retention timeframe expires, the charity must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the charity's management team. The charity specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is particularly forbidden, or destroying data in an attempt to cover up a violation of law or charity policy.

4.6 Applicability of Other Policies

This document is part of the charity's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the directors of the charity and by the executive director. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of charity property (physical or intellectual) are suspected, the charity may report such activities to the applicable authorities.

6.0 Definitions:

Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption: The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.