Gwasanaeth
Cerdd Ysgolion
Gwynedd a Môn

Data Protection Policy

Policy Reference	**Pol_GCYGM_7S**
Version	**2**
Last Approval / Review Date	**April 2025**
Next Review Date	**April 2028**
Uncontrolled document once printed	

1. INTRODUCTION

1.1 The main objective of the Gwynedd and Anglesey School Music Service (GCYGM) is to promote and encourage musical activity in Wales particularly by promoting expressive art and music in the context of dance, drama, poetry, television and film. This is achieved through our provision of instrumental music and vocal lessons to around 5,000 pupils by over 50 experienced tutors, our musical instruments lending service and the regional and county ensembles.

2. PURPOSE

2.1 We take the privacy of personal data and other information seriously; we are registered with the Information Commissioner's Office (ICO) under the registration number – Z869229X.

2.2 This data protection policy sets out how GCYGM ("we", "us") handle the personal data of our customers, individuals who receive a service, suppliers, employees, workers, sub-contractors and other third parties.

2.3 This policy aims to ensure that we have effective processes in place to protect any information given to us. We are committed to ensuring that privacy is protected. Should we ask anyone to provide certain information by which they can be identified, then they can be assured that it will only be used in accordance with this policy.

3. SCOPE

3.1 This data protection policy applies to all personal data that we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, individuals who receive a service or supplier contacts, website users or any other data subject.

3.2 This data protection policy applies to all company personnel, who must read, understand and comply with this data protection policy when processing personal data on behalf of GCYGM. This data protection policy sets out what we expect in order for us to comply with applicable law. Compliance with this data protection policy is mandatory, any breach of this data protection policy may result in disciplinary action.

4. GENERAL DEFENITIONS

4.1 What is data protection?

4.1.1 Data protection aims to protect an individual's rights to privacy by regulating how organisations obtain, store and use their personal data. Data protection rules provide individuals with certain rights whilst also imposing certain duties and obligations on organisations. Young people and adults have the same data protection rights under the law.

4.1.2 We are committed to processing data in accordance with our responsibilities under the General Data Protection Regulation (GDPR), which is overseen and regulated by the Information Commissioners Office (ICO). Amongst other matters, the ICO:

- keeps a central record of those organisations that are formally registered with it
- provides further Guidance regarding particular issues e.g. marketing, fundraising etc.
- enforces the law through fines and prosecutions

4.2 Personal Data Protection Principles

4.2.1 We adhere to the principles relating to processing of personal data set out in the GDPR

which require personal data to be:

(a) Processed lawfully, fairly and in a transparent manner.

(b) Collected only for specified, explicit and legitimate purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

(d) Accurate and where necessary kept up to date.

(e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

(g) Not transferred to another country without appropriate safeguards being in place.

(h) Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4.2.2 We will maintain a full Data Asset Register which will list all of the data assets we hold in order to fulfil our organisational purposes. We may use personal data for internal organisational purposes including, without limitation, to:

(a) improve the content and provision of lessons, courses, concerts and other related activities
(b) process applications for lessons
(c) process admissions to courses
(d) organise lessons, courses, concerts, regional and county ensembles, tours and events
(e) administer the regional and county ensembles
(f) raise funds
(g) administrate membership records
(h) promote the music service through public relations and marketing
(i) enforce our terms and conditions and payment procedures and collection
(j) and in any other reasonable manner in order to carry out our organisational objectives or to provide a specific service

POLICY DETAIL

5. Lawfulness, fairness and transparency

5.1 <u>Lawfulness and fairness</u>

5.1.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. We may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes.

5.1.2 These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the data subject has given his or her consent;

(b) the processing is necessary for the performance of a contract with the data subject;

(c) to meet our legal compliance obligations;

(d) to protect the data subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

5.2 Consent

5.2.1 We will seek the data subjects consent to processing of their personal data.

5.2.2 Data subjects can withdraw consent to processing at any time and withdrawal will be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

5.3 Transparency (notifying data subjects)

5.3.1 In line the GDPR, we provide detailed, specific information to data subjects through appropriate privacy notices which are concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

5.3.2 Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we provide the data subject with all the information required by the GDPR including the identity of the data controller, how and why we will use, process, disclose, protect and retain that personal data by way of a fair processing notice which is presented when the data subject first provides the personal data.

5.4 Purpose limitation

5.4.1 Personal data will only be collected for specified, explicit and legitimate purposes and will not be further processed in any manner incompatible with those purposes.

5.4.2 If data is used for new, different or incompatible purposes from that disclosed when it was first obtained, we will inform the data subject of the new purposes and ask their consent where necessary.

5.5 Data minimisation

5.5.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

5.5.2 You may only collect personal data that you require for your job duties: we will not collect excessive data and do not make unnecessary copies, and will ensure any personal data collected is adequate and relevant for the intended purposes.

5.5.3 When personal data is no longer needed for specified purposes, it is deleted, securely destroyed or anonymised in accordance with data retention guidelines.

5.6 Accuracy

5.6.1 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

5.6.2 We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards, and we will take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

5.7 Storage limitation

5.7.1 Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed, this will be detailed on our Data Asset Register.

5.7.2 We will not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

5.7.3 We will take all reasonable steps to destroy or erase all personal data that we no longer require from our systems in accordance with all our applicable policies. This includes requiring third parties to delete such data where applicable.

6. Security integrity and confidentiality

6.1 Protecting Personal Data

6.1.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

6.1.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption where applicable). We will exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure. This includes:

(a) a prohibition on saving personal data to personal computers or other devices;

(b) seeking consent before any personal data is removed from the Company's premises;

(c) the use of strong passwords;

(d) locking computer screens;

(e) ensuring documents containing personal data and sensitive personal data are kept securely;

(f) encrypting data when electronically transferring it to other parties; and

(g) considering use of separate keys / codes to anonymise data so the data subject cannot be identified.

6.1.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

(b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

6.2 Reporting a Personal Data Breach

6.2.1 The GDPR requires data controllers to notify any personal data breach to the ICO and, in certain instances, the data subject.

6.3 Transfer limitation

6.3.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

6.4 Data subject's rights and requests

6.4.1 Data subjects have rights when it comes to how we handle their personal data. These include rights to:

(i) withdraw consent to processing at any time;

(j) receive certain information about the data controller's processing activities;

(k) request access to their personal data that we hold;

(l) prevent our use of their personal data for direct marketing purposes;

(m) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(n) restrict processing in specific circumstances;

(o) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(p) request a copy of an agreement under which personal data is transferred outside of the EEA;

(q) object to decisions based solely on automated processing, including profiling;

(r) prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(s) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(t) make a complaint to the supervisory authority; and

(u) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

6.4.2 We will verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

7. Accountability

7.1 We have adequate resources and controls in place to ensure and to document GDPR compliance, including:

(a) appointing officers and a Board Member accountable for data privacy;

(b) providing training on the GDPR; and

(c) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of tests to demonstrate compliance improvement effort.

8. Record keeping

8.1 The GDPR requires us to keep full and accurate records of all our data processing activities, this will be in the form of our Data Asset Register. We will also maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

9. Audit

9.1 We will regularly review all the systems and processes under our control to ensure they comply with this data protection policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

10. Direct Marketing

10.1 We are subject to certain rules and privacy laws when marketing to our customers. For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of providing a service to that person, and we are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

11. Sharing Personal Data

11.1 Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

11.2 We will only share the personal data we hold with third parties, such as our service providers if:

(d) they need to know the information for the purposes of providing the contracted services;

(e) sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;

(f) the third party has agreed to comply with the standards, policies and required data security procedures and put adequate security measures in place;

(g) the transfer complies with any applicable cross border transfer restrictions; and

(h) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

12. Review

12.1 GCYGM will regularly review this privacy policy, including a full review every three years.

Adopted by the GCYGM Board of Trustees on the: 10th of April 2025