North and Midlands School of Music

Data Protection Policy

Context and overview

Policy prepared by:	Stephen Thackeray
Approved by Management Committee on:	12/05/2018
Policy became operational on:	12/05/2018
Next review date:	12/05/2021

Introduction

The North and Midlands School of Music needs to gather information about individuals for the purposes of administering the School and to communicate with the membership of the School.

This policy describes how this data must be collected, handled and stored to meet the School's data protection standards and to comply with data protection laws.

Why this policy exists

This data protection policy ensures the North and Midlands School of Music:

- Complies with data protection laws and follows good practice
- Protects the rights of Members and the Management Committee
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The General Data Protection Regulations describe how organisations, including the North & Midlands School of Music must collect, handle and store personal information. These rules apply regardless of whether personal information is stored electronically, on paper or in any other format.

The eight principles of the General Data Protection Regulations state that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Be accurate and, where necessary, kept up to date
5. Not be held for longer than is necessary
6. Be processed in accordance with the rights of Data Subjects under the Act
7. Have measures in place to protect personal data from unauthorised access, accidental loss or damage
8. Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

People, risks and responsibilities

Policy scope
This policy applies to:

- The Management Committee of the North & Midlands School of Music
- Any third party company (e.g. printers of publications)

It applies to all data relating to identifiable individuals, even if that information falls outside of the Data Protection Act. This may include:

- Names of individuals
- Postal addresses
- Telephone numbers
- Email addresses
- Any other information relating to individuals

Data protection risks
This policy helps to protect the North & Midlands School of Music from very real data security risks, including:

- Breaches of confidentiality – e.g. information being given out inappropriately
- Failure to offer individuals the freedom of choice over how the School handles their data
- Reputational damage – e.g. if hackers obtain access to sensitive data

Responsibilities
Everyone who performs duties within the North & Midlands School of Music has some responsibility for ensuring data is collected, stored and handled appropriately.

However, these people have key areas of responsibility:

The **Management Committee** is ultimately responsible for ensuring the North & Midlands School of Music meets its legal obligations.

The **Data Protection Officer** is responsible for:

- Keeping the Management Committee updated about data protection responsibilities, risks and issues
- Reviewing data protection procedures and policies
- Handling data protection questions from Members, the Management Committee or anyone else covered by this policy
- Dealing with requests from individuals to see information the North & Midlands School of Music holds on them
- Checking and approving any contracts with third parties

The **IT Officer** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable standards
- Performing regular checks to ensure hardware and software meet security standards
- Evaluating third-party providers such as website hosting providers

The **Membership Secretary** is responsible for:

- Ensuring the membership database is kept up to date and free from error

Distributing publications and marketing materials to Members on behalf of the School

The **Bursar** is responsible for:

- Ensuring any personal information involved with the finances of the School is stored and processed appropriately within the scope of this document and the law.

The **Senior Executive Officer** is responsible for:

- Ensuring any personal information involved in examinations/assessments is stored and processed appropriately within the scope of this document and the law

The **Archivist** is responsible for:

- Storing archive material, and any personal data it contains, securely and safely in accordance with the guidelines in this document.

General Management Committee guidelines

- The only people able to access data covered by this policy should be those who require it for the work of the North & Midlands School of Music
- Data should not be shared informally, but requested via the Management Committee
- Members of the Management Committee should keep all personal data secure by taking sensible precautions and follow the guidelines below
- Strong passwords must be used for email and any electronic systems where data is stored
- Personal data must not be shared with unauthorised people, either inside or outside of the School
- Data should be regularly reviewed and, if out of date or no longer required, it should be deleted or disposed of in a secure manner

Data storage

These rules describe how and where data should be stored. Questions about storing data safely can be directed to the IT Officer or Data Protection Officer.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Paper and printouts **should not be left where unauthorised people could see them**.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored locally and should only be uploaded to an **approved cloud computing service** or emailed where necessary, taking precautions to ensure good security is maintained.
- Data should be **backed up frequently**. Those backups should be tested regularly.
- All servers and computers containing data should be protected by **security software and a firewall**.

Data use

Personal data is of no value to the North & Midlands School of Music unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, the Management Committee should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should, where possible, not be sent by email, as this form of communication is not secure.
- Data should be **encrypted (where possible) before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.

Data accuracy

The law requires reasonable steps to be taken to ensure data is kept accurate and up to date.

It is the responsibility of all of the Management Committee who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data should be held in **as few places as necessary**. The Management Committee should not create any unnecessary additional data sets.
- **Every opportunity should be taken to ensure data is kept updated.**
- It should be **easy for data subjects to update the information** the North & Midlands School of Music holds holds about them, either by phone or electronically.
- Data should be **updated as inaccuracies are discovered**. For instance, if a member's stored telephone number is found to be incorrect, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by are entitled to:

- Ask **what information** the organisation holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the North & Midlands School of Music requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at **dataprotection@nmsm.org.uk**. The Data Controller can supply a standard request form, although individuals do not have to use this.

The Data Controller will aim to provide the relevant data within 14 days.

The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the North & Midlands School of Music will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

The North & Midlands School of Music aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the organisation has a privacy statement, setting out how data relating to individuals is used by it.

This document was last updated May 2018