Live Music Now Scotland

Data Protection Policy

Introduction

Live Music Now Scotland (LMNS) needs to collect, gather and use certain information about individuals. These can include supporters, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

The information LMNS collects and holds is in order to deliver on its charitable objectives which are listed on OSCR as:

1 The advancement of the arts and culture through the promotion of music and other performing arts, in particular among those members of the public who would otherwise be deprived of the benefit of performances of live music and of other performing arts.
2 To advance the musical education of musicians at the outset of their careers as performing artists by providing them with support, specialist training and the opportunities to complete their practical education by performing and working in public.

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

This data protection policy ensures LMNS:

- complies with data protection law and follows good practice;
- protects the rights of staff, supporters and partners;
- 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The General Data Protection Regulation (GDPR) took effect as of 25th May 2018 and superseded the Data Protection Act 1998 (DPA). The regulation describes how organisations must collect, handle and store personal information and apply regardless of whether data is stored electronically, on paper or on other materials.

LMNS is committed to following the data protection principles to make sure any information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

The conditions for processing are set out in the Data Protection Act and didn't change with the introduction of the GDPR. Unless a relevant exemption applies, at least one of the following conditions will be met by LMNS and its employees whenever personal data is processed:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary:
    - in relation to a contract which the individual has entered into; or
    - because the individual has asked for something to be done so they can enter into a contract.

- The processing is necessary because of a legal obligation that applies (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". (This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.)
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

LMNS will NOT:

- collect and hold any personal data of the members of our audiences
- collect and hold any personal data of anyone under the age of 18
- hold any information once it's been requested to be deleted from our system (within a four-week admin period)
- give or sell our data to anyone else without the individual's consent.

Policy Scope

This policy applies to:

- All staff and freelance consultants ("employees" for ease of reference and clarity) and volunteers of LMNS.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR (this can include names of individuals, postal addresses, telephone numbers and email addresses, etc).

Data protection risks

This policy helps to protect LMNS from some very real data security risks, including:

- Breaches of confidentiality, i.e. information being given out inappropriately.
- Failing to offer choice, i.e. all individuals should be free to choose how the company uses data relating to them.
- Reputational damage, i.e. the company could suffer if hackers successfully gain access to sensitive data.

Responsibilities

Everyone who works for or with LMNS has some responsibility for ensuring data is collected, stored and handled appropriately.

Each time personal data is handled, employees of LMNS must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following groups have key areas of responsibility:

The **Board** is ultimately responsible for ensuring that LMNS meets its legal obligations

The **Director** is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Overseeing any contracts or agreements with third parties that may handle the company's sensitive data

The **General Manager** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data LMNS holds about them (also called 'subject access requests')
- Working with our external IT Partner to ensure data protection compliance is followed by them for our website, database and our cloud-based services
- Approving any data protection statements attached to communications such as emails and letters.

The **Communications Officer** is responsible for:

- Ensuring the necessary permissions are in place for any images used to promote LMNS activity
- Addressing any data protection queries from journalists or media outlets
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines

LMNS grants access permissions to certain records on a 'need to know' basis to its employees, i.e. for HR processing (for ease or reference and clarity 'employees' includes salaried staff and freelance consultants). All employees must follow the LMNS data protection principles, namely:

- Data should not be shared informally with anyone. When access to confidential information is required, employees must request access from their line managers.
- LMNS will provide training to all employees to help them understand their responsibilities when handling data.
- All employees should keep all data secure, by taking sensible precautions and:
    - using **strong passwords**. These are provided by LMNS for Office 365 and internal database logins. All laptops and computers should be password protected.
    - LMNS uses the password manager Bitwarden to maintain security with passwords. Employees will be given a user log in for Bitwarden and this should be used to safely store and complete log in information for any software/applications that are required in undertaking LMNS work. This should also be used to generate secure passwords for any new log ins required. Timing for vault lock should be set at a maximum of 5 minutes on any Bitwarden applications to ensure security.
    - **Personal data should not be disclosed** to unauthorised people, either within the company or externally.
    - **Data should be regularly reviewed and updated** if it is found to be out of date. If it is no longer required, it should be deleted and disposed of.
    - Employees should request help from the General Manager if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the General Manager.

LMNS runs a secure database connected to our website and expects all paper documents to be saved securely as a pdf within its password protected Sharepoint files. The LMNS database is housed on the cloud, has full SSL Certification and is password protected. Sharepoint files are shared with employees on a 'need to know' basis.

As a rule, data should be safeguarded as follows:

- All files should be saved within the password protected Sharepoint folders. If they are in paper copy then they should be scanned so they can be electronically saved.

All paper files should be kept to a minimum. Where necessary they should be protected accordingly:

- Paper or files should be kept in a locked drawer or filing cabinet when not required
- Paper and printouts should not be left where unauthorised people could find them, like a printer
- Data printouts should be shredded and disposed of securely when no longer required

LMNS's electronic data is housed securely in the cloud via our IT Services Partner and safeguards include:

- All employees should use strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or memory pen) these should be kept locked away securely when not in use.
- Data should only be stored on designated systems, drives and servers and uploaded onto the approved cloud based systems.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All computers and laptops used for work purposes should have the latest security and firewall software installed.

Data Use

Personal data is of no value to LMNS unless the charity 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 so employees should:

- ensure, when working with personal data, that the screens of their computers are always locked when left unattended.
- not share personal data informally: employees should access this information via the secure database.
- never transfer personal data or give it to anyone outside of the organisation.
- always access and update the central copy of any data and should NOT save copies of personal data to their own computers.

Data Accuracy

The GDPR requires LMNS to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in the centralised database to reduce duplication

- LMNS will make it easy for data subjects to update their information via the website and contact email address
- Data should be updated as inaccuracies are discovered. For instance, if a contact can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

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

- ask what information the company 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.
- request a copy of this information.
- request the right to be forgotten.

Individuals may request, via email to info@livemusicnow.scot, to obtain copies of the information LMNS stores in electronic and paper form. LMNS will not charge for these requests but reserves the right to charge a reasonable fee should the request be manifestly excessive or unfounded, particularly if it is repetitive. Requests should be made for the attention of the General Manager and, once the identity of the individual has been verified, LMNS will aim to provide the relevant data within four weeks.

Data Breach

In the unlikely event that LMNS suffers a data breach, the charity undertakes to advise all affected individuals as quickly as possible as to what information has been taken and when.

Disclosing data for other reasons

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

Under these circumstances, LMNS will disclose the requested data. However, LMNS will ensure the request is legitimate with the Director seeking assistance from the Board and the company's legal advisers where necessary.

Providing Information

LMNS 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, LMNS has a Privacy Statement, setting out how data relating to individuals is used by the company. This is available on request and a version of this statement is also available at www.livemusicnow.scot

Contact

If you have any questions regarding LMNS's Data Protection Policy, or other concerns over privacy, please email the General Manager at info@livemusicnow.scot who will be happy to discuss this further.

This policy was last reviewed on 3 August 2021.

Carol Main, Director **Date 31/8/2021**