Digital Safeguarding Policy

Purpose and Scope

Safeguarding is at the heart of everything we do at Music For Youth.

We have a responsibility to protect and promote the safety and wellbeing of young people as we help them reach their full potential through music.

We are committed to the welfare and safeguarding of all our participants, volunteers and staff both offline, and online. And as part of this we believe it's important we can demonstrate best practice in digital safeguarding.

This policy sets out the expectations for all Music For Youth's participants, volunteers, staff, associated contractors, third party providers and users to ensure the protection of children, young people and volunteers and staff online.

As volunteers, participants, volunteers and staff of Music For Youth it is our responsibility to raise concerns and report online incidents that happen inappropriately, using this policy and its procedures.

Music For Youth's commitment to digital safeguarding

Music For Youth is committed to safeguarding our participants, volunteers and staff – and it is our policy to apply the same rigorous level of safeguarding protection to online as we do in person.

Additional safeguarding measures are put in place to minimise specific online risk.

Who is this policy for?

This policy is for participants, members, volunteers, staff and all users of Music For Youth online services, website and platforms.

What does this policy cover?

This policy specifically covers all Music For Youth online and digital activities, plus all digital activities undertaken on behalf of Music For Youth at a national, international, and regional level, on proprietary platforms (i.e. non-Music For Youth affiliated) and third-party social media and devices.

This includes but is not limited to email; social media channels (such as Facebook, Twitter, YouTube, Instagram, WhatsApp, TikTok, LinkedIn); all blogging platforms; volunteer platforms; and other digital platforms such as Google Hangouts, Zoom and Microsoft Teams; all ICT devices (including phones) and internet connectivity that is provided by Music For Youth.

This policy explains our approach to protecting participants, volunteers and staff. We are constrained by the terms of service of third-party social media providers in our approach. We promote safe use, but we also recognise that some issues will only be able to be handled by the service provider and the user themselves.

Music For Youth digital safeguarding principles

In order to uphold these principles our volunteers, participants and staff must:

- Ensure that social media accounts are set up appropriately.
- Make it clear on personal social media accounts using disclaimers that their views, thought and opinions are personal and not reflective of Music For Youth policies, procedure or guidance.
- Make sure that technical solutions are in place to reduce access to inappropriate content on devices owned or used by Music For Youth. These could be filtering or monitoring software for example parental controls.
- Ensure the correct permissions are in place before taking and using photographs on mobile devices.
- Delete pictures after the event and in accordance with the Music For Youth privacy policy.
- Make sure that they have parental permissions before contacting any young person under 18 years of age, even if they have contacted you first.

- Make every effort to ensure that young people understand why and how they must use social media responsibly and safely using the appropriate privacy settings.
- When submitting video content, participants are asked to confirm the following:

> **'In submitting this content, I declare that I have the permission of all parents, guardians and carers to sign on their behalf in respect of the terms and conditions noted for children aged 18 and under I also have their written consent'**

We recognise that digital safeguarding is an important part of all our work, and we are committed to always delivering best practice.

We will:

- Ensure our projects, activities, programmes and campaigns support all of our participants, volunteers and staff to stay safe online.
- Use best practice digital safeguarding for technical solutions, processes and procedures.
- Help our volunteers to support members in being effective online.
- Take best practice action when a digital safeguarding incident occurs.
- Support and train appropriate volunteers and staff in digital safeguarding.
- Risk-assess all projects, initiatives, programmes, activities, services and campaigns to make sure appropriate digital safeguards are in place.

Who is responsible for digital safeguarding across Music For Youth?

The Operations Team leads digital safeguarding in Music For Youth and work with the IT Team. As a participant, volunteer, or staff member, if you know of an allegation, concern or disclosure incident you must inform Music For Youth.

When an incident happens or a participant raises an issue at an online meeting, you must deal with it the same way as other safeguarding incidents. If you aren't sure about how to handle incidents you should contact the Operations Team at mfy@mfy.org.uk

Music For Youth is committed to the protection of our participants, volunteers and staff and will only share information with other agencies where there are significant concerns, or a potential crime has been committed.

What do we mean by digital safeguarding?

Digital safeguarding means: 'the protection from harm in the online environment through the implementation of effective technical solutions, advice and support and procedures for managing incidents'. Music For Youth is committed to the safeguarding and protection of all participants, volunteers, staff and users of our digital services and social media channels, and we apply the same safeguarding principles to Music For Youth activities whether they are offline or online.

This means protecting our members, volunteers and staff from online harms such as:

- Online bullying and harassment
- Sexual exploitation and grooming online
- Discrimination and abuse on the grounds of any protected characteristic
- Sharing of illegal and inappropriate imagery
- Cyberstalking
- Impersonation and hacking
- Disinformation and misinformation
- The oversharing of personal information