Love Music Digital Safeguarding Policy

Adopted: 3rd Dec 2025, Review due: 1st Apr 2027

Digital Safeguarding Policy

Contents:

Definitions

Child / children: these terms are used to refer to individuals under the age of 18 years.

Vulnerable adults: this term refers to individuals who are aged 18 and over, who are or may be unable to protect themselves from harm due to age, illness, disability, or other impairment. These individuals may be at increased risk of abuse, neglect, or exploitation, including in digital spaces and online.

All participants: this term is used to refer to individuals who are taking part in Love Music's programmes and projects at any age. This may cover the groups defined above.

Love Music personnel: refers to all adults who represent Love Music including: office and production staff, management and trustees, freelance musicians, project staff, workshop leaders, trainees, volunteers and collaboration partners working in a Love Music capacity.

Policy Statement

The purpose of this statement is to:

- ensure the safety and wellbeing of all participants is paramount when participants use the internet and social media to access Love Music materials;
- provide staff and volunteers with the overarching principles that guide our approach to online safety;
- ensure that, as an organisation, we operate in line with our values and within the law.

Love Music Digital Safeguarding Policy

This policy statement applies to all Love Music personnel and all participants.
The policy sits alongside Love Music's Child Protection and Safeguarding policies, and once this policy is board approved it will be available on the Love Music website.

Our Commitment

Love Music acknowledges its responsibility to safeguard and promote the welfare of all participants, including children and vulnerable adults. Love Music is committed to ensuring that its safeguarding practice reflects statutory responsibilities, the guidance of young people's services and of the Scottish and UK Governments.

Love Music works with participants through its weekly choir programmes, and in wider schools and project-based work. This work includes digital elements, including access for online choir participants and online access to resources, marketing and collaboration tools. Our ability to provide a safe environment online is fundamental to our commitment to provide high-quality inclusive musical experiences that enable our participants to thrive.

We recognise that:

- while the online world provides people with many opportunities, it can also present risks and challenges;
- we have a duty to ensure that all participants involved in our organisation are protected from potential harm online;
- working in partnership with children and their parents or carers, vulnerable adults and their carers, and other agencies is essential in promoting welfare and in helping all participants to be responsible in their approach to online safety;
- all people, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Monitoring of policy, action plan & procedures

Love Music's safeguarding documents and practices will be reviewed every year, and in the following circumstances:

- changes in legislation and/or government guidance;
- as required by the government, Local Safeguarding Children Board, Local Authorities or children's services;
- as a result of any other significant change or event.

Digital Safeguarding Procedures

Love Music has a duty of care to the children, adults and communities we work with, as well as to our personnel. This document discusses the following areas of safeguarding, including the procedures to which all personnel must adhere to ensure a safe learning environment for all participating in a Love Music project:

1. Legal Framework
2. Forms of harm
3. Where digital safeguarding incidents may occur for an organisation
4. Responding to signs of abuse
5. Love Music's Devices

1. Legal Framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in Scotland including Protecting Scotland's Children and Young People – National Policy 2023, UNCRC (Incorporation) (Scotland) Act 2024 and GIRFEC 2023 update and the Adult Support and Protection (Scotland) Act 2007.

Summaries of the key legislation and guidance are available on:

- online abuse
- bullying
- child protection

In its working practices, Love Music employs individuals for work on projects involving children and vulnerable adults in line with the instructions of Protecting Vulnerable Groups (PVG) Scheme, managed by Disclosure Scotland.

2. Forms of harm

The NSPCC defines online abuse as any type of abuse that happens on the internet, using technology like computers, tablets, mobile phones, games consoles and other internet-enabled devices.

Children and vulnerable adults may experience several types of abuse online, including:

- **Cyberstalking:** Repeatedly using electronic communications to harass or frighten someone. For example, by sending threatening messages.
- **Discrimination and abuse on the grounds of protected characteristics:** It can be an offence to stir up hatred 'inciting hatred' on the grounds of any of the protected characteristics.
- **Disinformation:** Deliberate intent to spread wrong information.
- **Hacking:** Accessing or using computer systems or networks without authorisation, often by exploiting weaknesses in security.
- **Harmful online challenges:** Online challenges sometimes show people doing dangerous things. People share these posts on social media, encouraging others to do the same.
- **Hoaxes:** A lie designed to seem truthful.
- **Impersonation:** Where someone pretends to be someone else online. This is often by taking photos from social media to build a fake profile. This is sometimes known as 'catfishing'.
- **Misinformation:** Where someone shares information they think is correct, but isn't.
- **Online bullying:** Offensive, intimidating, malicious, insulting behaviour and abuse of power online. This can humiliate or denigrate people.
- **Online harassment:** Unwanted contact online intended to violate someone's dignity. It could be hostile, degrading, humiliating or offensive.
- **Promotion of self-harm, suicide and eating disorders:** Content encouraging these harmful behaviours on social media.
- **Radicalisation:** Radicalisation aims to inspire new recruits, embed extreme views and persuade vulnerable people to support a cause. This may be through a direct relationship or through social media.
- **Sexual exploitation and grooming online:** Developing a relationship with a child with the intention of abusing them. Offenders use emotional and psychological tricks to build relationships. The abuse can take place online or offline.
- **Sharing of illegal and inappropriate imagery:** 'Illegal' means child sexual abuse imagery and imagery that incites violence, hate or terrorism. 'Inappropriate' could mean sharing pornography, or violent or hateful content.
- **Oversharing personal information:** This includes information that makes someone identifiable, like their names, address or phone number. It may also include identifying details based on someone's protected characteristics.

Children and adults may also be exposed to other online harms, such as inappropriate behaviours or content online.

3. Where digital safeguarding incidents may occur for an organisation

A digital safeguarding incident can occur anywhere across an organisation's digital footprint. A digital footprint is a unique set of digital activities, actions, and communications that can identify an organisation online. It can be extremely broad because it comprises everything the organisation has said and everything others have said about the organisation – not all of a digital footprint is under the control or influence of the organisation itself. A digital footprint can include, but is not limited to, content that can be found via:

- Organic search through a search engine such as Google, or a social media platform
- Directories, event platforms and review sites
- Social media or social sharing
- Influencers and affiliates
- Blogs
- Marketplaces
- Brand Partnerships
- PR
- Online activities including events, workshops and meetings

In addition to the 'official' digital footprint of an organisation – that is, content created at the direction, or with the endorsement of the organisation – there exists significant potential for a large 'unofficial' digital footprint to exist. This 'unofficial' footprint includes genuine user-generated content (such as reviews or posts in networking groups) and illegitimate content. Unofficial content, in whatever form, poses significant Digital Safeguarding risks.

The greatest Digital Safeguarding risk is posed by social media. Social media refers to digital platforms that provide such services as blogs, discussion forums and instant messaging. Social media includes, but is not limited to:

- Social networking sites, eg. Facebook
- Micro-blogging services, eg. X
- Video-sharing services, eg. YouTube
- Photo-sharing services, eg. Instagram
- Social media platforms often incorporate more than one of the features listed above alongside their primary services.

Examples of popular social media sites include, but are not limited to: LinkedIn, Facebook, X, YouTube, Instagram, Snapchat, Flickr, TikTok, Yammer, Yahoo/MSN messenger, Wikis and blogs, Weibo, WeChat and WhatsApp.

While Love Music do not actively moderate user content unless a user specifically interacts with us online, we will generally monitor our digital footprint and will report or remove user content which could be deemed a digital risk, in line with both our safeguarding and our data protection policies and procedures.

We will ensure that all online services we use and access are protected with strong, secure passwords and, where available, two factor authentication is used.

When devising programmes, events and resources for participants to access, we will conduct a risk assessment on the most secure and protective ways to share information and content online.

4. Responding to signs of abuse

In general

- Stay calm.
- Remember that the safety of the child or vulnerable adult is paramount.

Following suspicions

The guidelines for Love Music personnel suspicious of online abuse are as follows:

- If you think someone is at risk of harm, you must report it.
- Make a note of what you have witnessed, along with the response, in case there should be any consequences in which you may be involved (see incident form). Do not investigate or take matters into your own hands.
- Speak to the Designated Person / Child Protection Officer about your concerns immediately so that action can be taken, and both you and the individual concerned can be protected.

If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse – see the procedures at the end of this document.
- Providing support and training for personnel on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response considers the needs of the person experiencing abuse, any bystanders and our organisation as a whole.
- Reviewing the plan developed to address online abuse at regular intervals, to ensure that any problems have been resolved in the long term.

Exposure to child sexual abuse images

If a member of Love Music personnel is exposed to child sexual abuse images of children whilst using the internet in the course of their duties, they should report it as below:

- The URLs (webpage addresses) which contain the suspect images should be reported to the Internet Watch Foundation via www.iwf.org.uk and the Child Protection Officer should be informed at that time or as soon after as is reasonably possible.
- If these images are found on any Love Music websites, you should refer to the Child Protection Officer who will carry out the report. Love Music must not send copies of the images to the Internet Watch Foundation.
- Any copies that exist of the image, for example in emails, should be deleted. The Managing Director should arrange for IT support to ensure the deletion process is complete.

Abusive Images

If abusive images of children are found on Love Music's devices but it's not clear who was responsible for uploading them:

- You must report what you have seen to the Child Protection Officer within 24 hours and if unavailable contact another senior member of Love Music staff.
- If relevant, the URLs (webpage addresses) which contain the suspect images should be reported on to the Internet Watch Foundation via www.iwf.org.uk by the Child Protection officer. You must not send copies of the images to the Internet Watch Foundation.
- The police should be informed, and the Incident Form completed.

- If any copies of images need to be stored at the request of the police, then they should be stored securely where no one else has access to them. The Managing Director should agree a plan for storage, as advised by the police, in agreement with Trustees.
- All other copies must be deleted by the Managing Director.
- The Child Protection Officer and the police together will further investigative action if necessary.

5. Love Music's Devices

If a member of Love Music personnel is found in possession of child sexual abuse images on any electronic device provided by Love Music:

- You must inform the Child Protection Officer and if unavailable contact a Designated Person on the project, or a Trustee.
- If there is a doubt about whether the images are criminal, the Child Protection Officer should contact their Local Authority Designated officer at the City of Edinburgh Council Children and Families' Social Work team (Social Care Direct) by calling **0131 200 2327** who will advise.
- If a referral is required, the Child Protection Officer should complete the City of Edinburgh Council Social Care Direct referral form as relevant to the area of work.
- The Child Protection Officer to agree with Social Care Direct what to do about the device that the images are on.
- Quarantine the device in question and discuss with Social Care Direct about checking for any other images on that device or any others.
- Instigate the arrangements for managing allegations against a member of Love Music personnel.

If a participant discloses that they are being groomed, abused or bullied online:

- Follow the procedures outlined at the end of this document.
- The Child Protection Officer should contact the police. Advice and a report can also be made to **CEOP** which is a specialist police command dealing with inappropriate online behaviour.
- If the person committing grooming is Love Music personnel, the Child Protection Officer should follow the procedure as outlined in the Child Protection Policy.

Contact Information: The Child Protection Officer & Designated Person

Love Music's Child Protection Officer is Ruth Davie, Managing Director. All incidences, suspicions and disclosures must be reported to them and they will liaise with the authorities using the information reported. This includes incidents relating to all participants even if over the age of 18.

Contact: ruth@lovemusic.org.uk 07806604044

The Designated Person is the project manager or workshop leader present when the Child Protection Officer is not present. This might be an employed project manager or producer, the Artistic Director or a trained member of the board of Trustees.

The Child Protection Officer receives regular training and notifications from the NSPCC and the Protecting Vulnerable Groups Scheme to keep up to date with safeguarding procedures.

When the Child Protection Officer is not present for a project, all concerns, disclosures and allegations must be communicated to them at the earliest opportunity, but in the first instance should be shared with the project's Designated Person (who will pass on your report). Personnel will be informed as to the identity of the Designated Person (eg. the project manager) via their schedules.

The role of the Designated Person is to:

- be the first point of contact for reporting allegations, disclosures and concerns of abuse;
- receive information from Love Music personnel, participants or participants' parents or carers who have concerns, and ensure they have recorded the details (see incident report template below for details to record);
- pass on reports to the Child Protection Officer.

The role of the Child Protection Officer (regarding this Digital Safeguarding Policy) is to:

- lead on making a formal referral to the appropriate authorities and senior management, act as a source of advice, support and knowledge within the organisation;
- ensure that all Love Music personnel are aware of and have access to this document;
- work closely with staff and trustees to inform of any arising issues and address these with best practice;
- ensure that the policy and associated documents are updated regularly;
- ensure that accurate and secure written records of referrals are kept;
- store and retain child protection records according to legal requirements and the organisation's safeguarding and child protection policy and procedures;
- keep a record of all contact details of all authorities so they can be contacted should any suspicion, allegation or referral occur;
- keep up to date with legislation and guidance changes, training, and the regular training and practice of Love Music personnel.

It is not the role of the Designated Person or Child Protection Officer to decide whether a child, vulnerable adult or participant has been abused or not; this is the task of the relevant authorities. However, it is everybody's responsibility to ensure that concerns are shared, and appropriate action taken.

Related policies & procedures

This policy statement should be read alongside Love Music's organisational policies and procedures, including:

- Child Protection Policy
- Safeguarding Policy (covering all participants over 18)
- Privacy Policy
- Data Protection Policy
- Cyber Security Policy
- Health and Safety Policy
- EDI Policy
- Board Member's Code of Conduct

These are available on request and via the staff handbook.

Other relevant information contacts & resources

- NSPCC Helpline 0808 800 5000 for advice. Open 24/7 all year round.
- Child Exploitation and Online Protection (CEOP): CEOP Safety Centre www.ceop.police.uk/Safety-Centre/
- 999 (emergency) / 101 (non-emergency) for the Police
- Children's services: Social Care Direct Edinburgh 0131 200 2327 / socialcaredirect@edinburgh.gov.uk **/** www.edinburgh.gov.uk/social-care-health/ask-social-care-direct-advice-2/3
- Children First Edinburgh www.childrenfirst.org.uk/get-support/how-we-can-help/local-services/edinburgh
- Duty to refer to the Protecting Vulnerable Groups scheme at Disclosure Scotland www.mygov.scot/organisations/disclosure-scotland

Sources for the creation of this document

NSPCC website www.nspcc.org.uk

'Working Together to Safeguard Children' (2013) HM Government

'What to do if you're worried a child is being abused' (2006) HM Government

Referral Procedure

Child or vulnerable adult discloses abuse / member of staff suspects abuse

↓

Staff member reports disclosure / concerns to the Designated Person for child and vulnerable adult protection

↓

Staff member records the nature of the disclosure / concerns using the pro-forma below

↓

Child Protection Officer makes referral to social work / police or other relevant agency and seeks advice on how to manage the immediate situation particularly in relation to the parents / carers and the child, or in situations regarding vulnerable adults

↓

Having obtained guidance from the statutory agencies, appropriate and sensitive support is offered to the individual concerned and, where appropriate, their parents/carers.

Incident Disclosure Form

Date of Incident:	
Time of Incident:	
Place of Incident:	
Names of all children and adults involved (including witnesses:	
What was seen, said or done and by whom? Stick to the facts (indicating which are your own and which are a young persons)	

Signed: Date:

Your contact details should the police or another authority need to follow up your report:

Phone: Email:

A record of this report will be stored securely, shared with authorities and organisations as is necessary to ensure the welfare of the individual concerned, but otherwise kept confidential.

TO BE COMPLETED BY THE CHILD PROTECTION OFFICER

Action taken by the designated person, CPO and organisations involved:	
Any further action taken:	
Referral to relevant statutory agency (indicate which and when):	
If relevant, the reasons for the decision not to refer to a statutory agency:	

Signed (CPO): Date: