

Digital Safeguarding Policy

17 December 2021 Next review: December 2022

Scope and Purpose

The International Teaching Artist Collaborative (ITAC) is the first worldwide network of artists who work in community and educational settings. ITAC teaching artists regularly work with children and adults who are potentially at risk for a variety of reasons.

The purpose of this policy is to:

- Ensure the safety and wellbeing of children and adults at risk of harm is paramount when children and adults are using the internet, social media, or mobile devices.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, ITAC operates in line with our values and within the law in terms of how we use online devices.

This policy applies to all staff and teaching artists who work for ITAC, whether on a permanent, temporary, commissioned, or voluntary basis. We also require that any partner organisations or artists working in association with ITAC be made aware of this policy and state their commitment to operate within it.

This document must be read in parallel with ITAC's Safeguarding Policy and Social Media Policy.

Legal framework

ITAC is a UK-based charity. This policy is therefore informed by the following legislation and guidance:

- United Nations Convention on the Rights of the Child (UNCRC)
- Equality Act (2010)
- The Care Act (2014)
- General Data Protection Regulation (GDPR) (2018)
- Data Protection Act (2018)
- Keeping Children Safe in Education (2021)
- Creating Safety: Child Protection Guidelines for Scotland's Art, Screen and Creative Industries (2019)
- National Guidance for Child Protection Safety in Scotland (2021)
- Communications Act 2003
- Digital Economy Act 2017
- NSPCC Undertaking Remote Teaching Safely

- National action plan on internet safety for children & young people (Scotland)

ITAC believes that:

- Children and adults at risk of harm should never experience abuse of any kind
- Children and adults at risk of harm should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

ITAC recognises that:

- The online world provides everyone with many opportunities but it also presents risks and challenges.
- We have a duty to ensure that all children and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep children and adults at risk of harm safe online, whether or not they are using ITAC's network and devices.
- All children and adults at risk of harm, regardless of their gender identity, ethnicity, disability, sexual orientation, age, language, economic status or religion, have the right to equal protection from all types of harm or abuse.

ITAC seeks to keep children and adults at risk of harm safe by:

- Appointing a designated safeguarding staff member (see below).
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults (see below).
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.
- Ensuring that user names, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing resources for staff and volunteers about online safety. Eg <u>Creating Safety | Creative Scotland; Statistics on child abuse | NSPCC Learning</u>
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation. Eg checking the age rating and access rules for streaming/gaming apps.

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

- Having clear and robust safeguarding procedures in place for responding to abuse (see below)
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.

- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Key contacts

Designated Safeguarding Staff Member: Madeleine McGirk, Managing Director

E.: madeleine@itac-collaborative.com | T.: +447739 411641

Designated Safeguarding Leadership Committee Member: Simon Sharkey

E.: simon@thenecessaryspace.com | T.: +4477889 625155

*Refer to <u>ITAC's Safeguarding Policy Reporting Structure (6.4)</u> for steps to take in the event of suspected or observed online abuse.

ITAC's Code of Behaviour (online/digital)

To be read in parallel with ITAC's Safeguarding Policy and Code of Behaviour

Working remotely:

When working remotely, core employees and freelancers will have their own accounts to access emails and a log-in to access files. All files are saved on the company's shared drives in files with access to personal contact details restricted to core employees only

- Employees will not share their accounts or log-ins with other members of staff, only logging into their own accounts, unless approved by ITAC's Managing Director
- No young people's details or images will be downloaded or saved on employees' computers (unless it is a computer provided for work use only).
- If young people's images need to be downloaded for photograph or video editing, then they will be deleted once the edit has taken place and the edited film is uploaded to the company's server.
- Teaching artists who share creative content including videos featuring young people shall provide links which enable people to watch videos online but not download.
- Employees will always lock home computers/laptops or close documents with sensitive information when they are away from their devices.

Communication via email:

When communicating via email, employees should always communicate with Teaching Artists and project participants via a company email account. Clear language must be used to avoid any misunderstanding on the part of the recipient. It may be appropriate to copy in another employee for transparency. Employees or freelancers who have concerns regarding the content of an email that they send or receive from a young person or an adult at risk of harm should consult the Designated Safeguarding Staff Member as named above.

Communication via social media

ITAC uses social media to communicate with its network of Teaching Artists (TAs) and a broader audience, which may include young people or adults at risk of harm. Current social media platforms employees may use include: Twitter, Facebook, Instagram and LinkedIn. Communication via such platforms should only take place through organisational accounts and should follow guidelines as laid out in the Social Media Policy. If an ITAC employee or freelance TA receives content via social media which they believe is inappropriate and indicative of abuse/a disclosure of abuse they will not forward the content or delete it but immediately contact the Designated Safeguarding Staff Member to report the content and follow the safeguarding incident procedure of the company (see main Safeguarding Policy).

Communication via digital platforms

When communicating with young people or adults at risk of harm via digital platforms, employees, freelancers, commissioned Teaching Artists and ITAC volunteers will use official accounts and ensure that the personal numbers of participants are not shared. When using video/call platforms with groups of young people, the following protocols should be followed:

- All platforms should be risk assessed in advance and those deemed appropriate for use should include mitigating measures. Risk assessments should be shared with all employees/freelancers who will be hosting sessions.
- Employees/freelancers should use high security settings and facilities of the selected platform to minimise the risk of third parties gaining access to sessions.
- In the case of online events or projects that involve young people, there will be a minimum of two adults present at every session.
- Employees and freelancers should be in a neutral area where nothing personal or inappropriate can be seen or heard in the background.
- Employees need to be present before young people or adults at risk of harm are invited to join an online meeting.
- When the meeting ends, the employees should eject each participant until only the employees remain and then close the call, thus ensuring no-one is left alone with a young person and no young people are left in a shared digital space unsupervised.
- In situations where one to one mentoring or creative development work takes place between a young person and an employee/freelancer, prior permission from parents/carers will be required and the meeting must be recorded when under 18.
- All meetings that are recorded require all participants' consent, regardless of their age, prior to the recording taking place. Employees/Teaching Artists must be specific about the reason for the recording and the way the recording will be used.
- Teaching Artists must inform all parents/carers of the platforms to be used and the dates and times of sessions and the adults who will be in these platforms.
- Employees will set clear rules of engagement for all who are working on digital platforms. These rules will be in line with the rules of the company when working in person (see Code of Behaviour in ITAC's Safeguarding Policy).

- Employees will also remind young people that this is not a private space and whatever they share online will be seen by the group and/or employees/freelancers working on the project.
- Any participant who breaks the rules that have been agreed between employees/Teaching Artists and the participants will be removed from the platform.

Receiving a disclosure online or via mobile phone

We recognise that at times, young people or adults at risk of harm might disclose information to employees via calls or digitally. If an employee receives a message that they think may indicate that the person communicating with them is at immediate risk, both during or outside of work hours, they should immediately refer it for action to the Designated Safeguarding Staff Member, ideally by speaking to them in person or by telephone. The Designated Safeguarding Staff Member will follow ITAC's safeguarding procedures. If the employee is unable to contact the Designated Safeguarding Staff Member, they should follow the procedure below:

- Check with the young person or adult at risk of harm: What is happening? Where are you? The employee should not attempt to solve the problem.
- Contact the young person's parent/guardian (if parental consent and contact details were required and the employee/Teaching Artist has access to this information). If there is no response, alert the emergency services (ambulance) and provide as much information as possible.
- Write up an incident report on the situation within 24 hours to be sent to the Designated Safeguarding Staff Member.

Sharing work created online

When sharing work created online that involves young people or adults at risk of harm, ITAC will take the following steps:

- Gain parent/carer consent for their child to be photographed and videoed for those under 18 years.
- Share the final edits of films with all participants and their parents/carers when under 18 where possible before sharing publicly.
- No use of a child/young person's surname in photography or video content unless requested.
- Only use images of children/young people in suitable clothing to reduce the risk of inappropriate use.
- Only share content through official accounts. If, for whatever reason, a parent/carer or young person is unhappy with the use of content, then the company will not share the content.

ITAC will review this policy annually.