



DIGITAL ENGAGEMENT & VIRTUAL LEARNING – SAFEGUARDING GUIDELINES

Introduction

As we move into 2021 SGM staff will be working more from home and with young people digitally. This document provides the guidelines for all workers to keep themselves and the young people they work with safe.

Digital Engagement work encompasses all the work The Stained Glass Museum team do to engage with audiences on digital platforms, including the museum's website and social media.

Virtual Learning encompasses both facilitated online and live streamed activities. These activities can either be private facilitated online sessions e.g., Virtual Classrooms for schools, or public sessions e.g. Museum talks. Platforms for these activities could include, Zoom, Microsoft Teams, Facebook Live and YouTube Live amongst others.

Included within this policy are the digital safeguarding guidelines below that must be adhered to.

Passwords to all our virtual learning and digital engagement platforms will be changed at least twice a year and accessed via a password-protected document.

This document should be read in partnership with Stained Glass Museum's (SGM) main Safeguarding Policy, and will be reviewed at least annually.

Designated Safeguarding Lead (DSL): Jasmine Allen,
Deputy Designated Safeguarding Lead (DDSL): David Whitney

Date this document was approved by the Board of Trustees: 22 February 2021

RESPONSIBILITIES

All staff, freelancers and volunteers delivering or helping to facilitate digital platform sessions or engaging on the museum's official social media accounts should read and abide by these guidelines.

It is the responsibility of the DDSL (the Learning & Community Engagement Manager) to ensure that guidelines are distributed as part of the induction and ongoing training of staff, freelancers and volunteers who may help use digital platforms to help deliver or facilitate the museum's remote learning programmes.

WORKING FROM HOME

When working from home staff will have their own accounts to access emails and a log-in to access files. All files are saved on SGM's encrypted Sharepoint and files with personal and contact details are password protected.

- No young people's details or images will be downloaded or saved on staff computers (unless it is a computer provided for work use only and correct procedures have been followed and permissions obtained).
- Staff will not share their accounts or log-ins with other members of staff and only log into their own accounts, unless working on the same document.
- If young people's images need to be downloaded for photo or video editing then they will be deleted once the edit has taken place and the edited film is uploaded to the SGM's server.
- Freelancers who need access to creative content including videos are given links which enable them to watch videos online but not download.
- Staff will always lock computer or close documents with sensitive information when they are away from their laptops / computers.

COMMUNICATION VIA EMAIL

Staff may be required to email young peoples' personal email addresses. Where possible we will CC in parents/teachers. In such cases staff will always use their work email account and should use clear language to avoid any misunderstanding on the part of the recipient. It may be appropriate to copy in another staff member for transparency. Staff members who have concerns regarding the content of an email that they send or receive from a young person should consult the DSL or DDSL for guidance.

COMMUNICATION VIA SOCIAL MEDIA

SGM will use social media during this time to communicate with children and young people. Current social media applications staff use include Twitter, Facebook, Instagram and YouTube. Contact with young people through such forums should only take place through organisational accounts. SGM will not follow young people's accounts and only invite members to follow SGM's accounts.

If a SGM staff member receives content from a young person which they believe is inappropriate they will not forward the content or delete it but immediately contact the DSL/DDSL to report the content and the DSL/DDSL will follow the safeguarding incident procedure of the company (see Safeguarding Procedures document.)

Current organisational social media accounts and the moderators for them are all trained members of staff who are familiar with this guidance and our Social Media Guidelines. The DSL holds details of staff users and moderators.

COMMUNICATION VIA DIGITAL PLATFORMS

When communicating with young people via digital platforms (e.g. Zoom, Microsoft Teams, Skype etc) staff will use official accounts and ensure that the personal numbers and email contacts of young people and freelancers are not shared.

Staff, freelancers and volunteers will be the only adults present in digital platform sessions and will have had a DBS check.

All parents/guardians and/or teachers will be informed of the digital platforms to be used and the dates and times of sessions and the adults who will be on these platforms.

Staff will set clear rules of engagement for working on digital platforms. These rules will be in line with the rules of the organisation when working in person.

Staff will also remind young people that this is not a private space and whatever they share online will be seen by the group. Where possible the young person will join an online meeting from a shared space, e.g. living or dining room and not a bedroom. The young person may also like to blur their backgrounds if they feel there is personal information about them in their environment. Any young person who breaks the above rules will be removed from the platform by staff and parents/carers will be informed.

RECEIVING A DISCLOSURE ONLINE OR VIA MOBILE PHONE

We recognise that at times, young people might disclose information to staff members via texts, calls or digitally.

If a staff member receives a worrying message that they think may indicate that the young person communicating with them is at immediate risk during or outside of work hours, they should immediately refer it for action to an executive staff member (DSL – Jasmine Allen 07799 218235 /DDSL – David Whitney - 07935 403 213), ideally by speaking to them in person (if the disclosure takes place in working hours) or by phone. The DSL/DDSL will follow the procedure below. If the staff member cannot get hold of the DSL/DDSL, or a more senior member of staff, they should also follow this procedure.

- Check with the young person by asking what is happening and where they are. The staff member should not attempt to solve the problem, just gather facts.
- Contact the young person's parent/guardian, or – if applicable – the social worker/key worker associated with that young person.
- If there is no response: Alert the emergency services (in most cases this will be the police) by calling 999 and giving as much information as possible.
- Write up an incident report on the situation within 24hrs to be sent to the DSL. Incident reports will be kept in the Learning folder under Safeguarding and will be password protected.

SHARING WORK CREATED ONLINE WITH YOUNG PEOPLE

When sharing work created online SGM will take the following steps;

- Share the final edits with the young people and their parents/carers before public sharing.
- No use of child's surname in photography or video content. See Safeguarding Policy [Point 7]
- Gain parental/guardian consent for their child to be photographed and videoed following our policy (as above).
- Only use images of children in suitable clothing to reduce the risk of inappropriate use.
- Only share content through official accounts.
- There will also be the option to withdraw from these permissions at any time.
- In the main data will be stored on our server for a maximum of 12 months in compliance with our GDPR policy.

If, for whatever reason, a parent/carer or young person are not happy with the use of content, then the museum will not share the content.

APPENDIX 1 - SAFEGUARDING FOR YOUNG PEOPLE WORKING DIGITALLY in Virtual Learning environments

These guidelines also to apply to when we are working with schools in accordance with their safeguarding procedures and will be sent out in advance of a session.

We want to work digitally to connect, create work and support each other. In order to do this we are going to use virtual learning environments and digital platforms. When using these platforms it is important to protect you and your families and follow our online code of conduct.

Before all virtual learning sessions participants will be advised of the following rules:

- Using Zoom: Each session will be password protected and the waiting room function will be switched on so that the host can monitor who is joining.
- When logging in, never use your full name, first names will do.
- When in the waiting room you will enter one by one with the session leader once your contact details have been cross-checked you will then join a separate breakout room with the session assistant. Once all members are in the breakout the room the session will then begin.
- Make sure people you are living with know you are on a live video chat. Don't include them in the chat.
- Wear appropriate clothing, even on parts of you that you think won't be seen.
- Please think carefully about your space/background and ensure that it is suitable for others to see. You may want to blur your background and remove personal items.
- Ensure that you are set-up, ready and comfortable before the start of session.
- Refer to a group leader directly if you feel worried about anything.
- Do not record or take photos of anything without the others consent.

During all virtual learning sessions, staff, freelancers and volunteers representing The Stained Glass Museum will ensure that:

- Two DBS checked adults will be present for the duration of every session; these will be designated as the session host and co-host.
- The host will only allow people to continue with the session if they have previously registered or signed up for it.
- The host will disable the chat function that enables members to chat between each other. However, participants will be able to post messages publicly and message the host. The chat will be monitored by the host and/or co-host.
- The host will be the only user able to share their screen and audio.
- If the host and co-host are leading the session remotely they will ensure that they are in an appropriate space/room, with an appropriate background (suitable for others to see and with any personal items e.g. photographs removed), and dressed appropriately (e.g. not in a bedroom, and dressed as they would be at work)
- The sessions will not be recorded. If recording needs to happen then the leader will seek consent. Videos will be deleted once they have served their purpose, and only shared with the appropriate permissions.

- SGM staff will only use SGM's official accounts for Virtual learning and digital engagement platforms.
- Where possible, e.g. for all public talks where face-to-face group interaction is not needed, attendees videos and mics will be disabled by the host, who will also ensure that a list of participants is not visible to all attendees.
- At the start of each live chat with young people, SGM's staff will establish a code of conduct / group contract for the session.

At the start of each session The Stained Glass museum staff will establish a code of conduct for working online that will include:

- Reminding young people that:
 - This is not a private space and not to do/share anything online that they would not do if the group were together
 - It is easy to misinterpret things online so be kind.
- Where possible the activity will be in a shared space and not a bedroom. Background should be blurred if the young person feels there is personal information about them in their environment. Young people should not be joined on screen by an adult unless they are a designated facilitator with appropriate DBS checks carried out by the museum.
- Participants should only attend an online meeting if their responsible adult has said they can, and if there is an adult in their immediate environment responsible for the young person.
- Introducing the platform technology to the group, explaining that everyone will have their microphones on mute when they are not speaking. Any 'raise your hand' / response features will also be introduced.
- Reminding participants that they must not record or take photos of anything during the session
- Reminding participants that any chat function is disabled and there will be no private chat between group members.
- Young people and parents/teachers/responsible adults will be advised about the process for reporting online abuse via CEOP (Child Exploitation and Online Protection), part of the national Crime Agency
<https://www.ceop.police.uk/safety-centre/>

If sharing work that was generated online The Stained Glass Museum will ensure that:

- The participant(s) we are sharing have given permission for videos/photography.
- The content we create will not reveal anything that might disclose the participant's home address/street.

If you are worried or concerned about anything online or personal during this period please contact The Stained Glass Museum staff they will listen and find you to the right support.



Jasmine Allen, Curator, Designated Safeguarding Lead -
07799 218235
curator@stainedglassmuseum.com

David Whitney – Learning & Community Engagement Manager,
Designated Deputy Safeguarding Lead 07935 403 213
learning@stainedglassmuseum.com

For Parents and Carers

Net Aware

<https://www.net-aware.org.uk/>

Online safety advice from Childline

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

Whether you're an online expert or you're not sure where to start, our tools and advice will help you keep your child safe.

ThinkUKnow

<https://www.thinkuknow.co.uk/parents/>

A website from National Crime Agency's CEOP Command about keeping children and young people safe on the internet.

UK Safer Internet Centre

<https://www.saferinternet.org.uk/>

Promoting the safe and responsible use of technology for young people.