Digital Writes - Development & Publishing C.I.C.

Remote Working and Online Video Workshop Guidelines

The purpose and scope of these guidelines

The purpose of these Guidelines is to ensure that the safety and wellbeing of children and young people is paramount when adults, young people and/or children are using remote communications and video conferencing to take part in our workshops, without jeopardising their creativity, productivity, personal development and fun.

This policy applies to anyone working on behalf of Digital Writes, including senior managers and the board of directors, paid staff, volunteers, freelancers, and students.

Supporting policies

These guidelines should be read close conjunction with our other organisational policies and procedures, in particular:

- Safeguarding Policy
- Online Safety Policy
- Privacy Policy
- Code of Conduct for Adults Working with Children and Young People
- Code of Conduct for Children and Young People
- Photography and Filming Policy
- Anti-Bullying Policy

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England:

- Child protection system in England by NSPCC: learning.nspcc.org.uk/child-protection-system/england
- 'Safe Remote Learning' by South West Grid for Learning (SWGfL): swgfl.org.uk/resources/safe-remote-learning
- 'Undertaking remote teaching safely' by NSPCC: learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely
- 'Guidance for working online, and online safeguarding' by the Culture, Health & Wellbeing Alliance, Arts Marketing Association, 64 Million Artists, and Real Ideas;

- ‘Safeguarding and remote education during coronavirus (COVID-19)’ by Department for Education: gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19
- ‘Video conferencing services: using them securely’ by National Cyber Security Centre: ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely
- ‘Video conferencing services: security guidance for organisations’ by National Cyber Security Centre: ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

We believe that:

- children and young people should never experience abuse of any kind;
- children young people should be able to use email, chat, messaging services, video conferencing and webinars for creative activities, education and personal development, but safeguards need to be in place to mitigate any risk.

Procedures for using email:

1. Where available, communicate with children and young people via their school email;
2. Only email children and young people from your digitalwrites.org.uk email which operates through a secure server;
3. Always cc another responsible adult:
    a. preferably a member of staff from the partner school, college or other organisation or institution;
    b. if not available, then another independent responsible adult;
    c. otherwise a senior member of Digital Writes’ staff;
4. Always cc a parent or carer if they have required this on their Consent Form;
5. NEVER use bcc;
6. If emailing with a child, young person or parent/carer about an allegation or complaint, always cc a senior member of Digital Writes’ staff;
7. Retain ALL emails with children and young people and members of staff from the partner school, college or other organisation or institution;
8. Keep emails organised using folders;
9. Try to keep email threads clear and clean so different discussions are discrete and easier to review;
10. In order to keep your emails organised, you may delete emails whose content and meta-data is contained within a later email reply, but do this with CAUTION;
11. The senior lead for safeguarding and child protection, Keith Phillips, will periodically rationalise, collate and securely archive concluded email conversations, in consultation with staff;
12. In all communications refer closely to the Code of Conduct for Adults Working with Children and Young People.

Procedures for using Digital Writes' website forums:

1. Digital Writes forums are set to "Private" which means only logged in participants are able to view the contents of the forums and they are not visible to the general public.
2. Children and young people are assigned logins by Digital Writes staff. This includes:
    a. an anonymising username agreed with the participant;
    b. a secure password;
3. The following formula creates strong passwords that are easy to remember:
    a. Aaaaa-Bbbbb-nn, where:
        i. Aaaaa is a five letter word, starting with a capital letter, strategically misspelled: such as "Agane".
        ii. Bbbbb is an unrelated five letter word, starting with a capital letter, strategically misspelled: such as "Basik".
        iii. nn is a number, as long or as short as you want.
4. You can create the password with the participant so it is something easy for them to remember.
5. Participants do not have access to their user profiles so are unable to add personal details or change their password. This keeps them and Digital Writes secure.
6. A member of Digital Writes' staff should monitor the forums at least daily. They should check:
    a. that discussions conform to our Codes of Conduct, Safeguarding Policy and related policies, in particular that:
        i. participants haven't revealed any personal details;
        ii. discussions are focused on the project;
        iii. discussions are friendly and mutually supportive;
        iv. there's no bullying.
    b. that there's nothing offensive.
7. Digital Writes staff should be scrupulous in adhering to the Code of Conduct for Adults Working with Children and Young People. Always be aware that anyone with an Immersive Authorship login can read what you're saying. In particular, if a participant needs individual support, continue that discussion via email.

Procedures for video conferencing:

Important notes:

1. With video conferencing you are essentially in students' homes, perhaps able to see details of young people's personal lives that would not normally be available to you.
2. Bear in mind that all of the information we gather (both consciously and unconsciously) from someone's environment informs our view of that person: their identity, social economic status, values and relationships.

3. Data use: How much data can you and the people you are working with afford? Some people have reliable broadband, some people rely on contracts or pay-as-you-go with mobile phone providers, which limit data use.
    - Consider whether you may be depriving people of data they could need for other things.
    - Consider the difference in data-use between software that relies on streaming video, software that uses images, and software that is mainly text-based.
4. This is a new space for us, and for most other people, and we will need to learn from each other as we go!

General Guidelines:

1. You must always have two responsible adults present at a Zoom meeting. This should ideally be:
    a. another Digital Writes employee, volunteer or intern who has been through our Induction Procedure (including safeguarding) and who has an Enhanced DBS Certificate;
    b. a teacher from a partner school.
2. Before the workshop:
    a. check your background for anything:
        i. that might be deemed unprofessional;
        ii. too personal;
        iii. that might identify your location if that is a concern;
    b. make sure the other people in your household are aware that you shouldn't be disturbed;
    c. make sure your computer has no personal or unprofessional material visible on your desktop or in open applications that you might inadvertently switch to when screen sharing.
3. Start the workshop by setting and discussing some of the goals that you are aiming to achieve, including:
    a. learning objectives, including:
        i. specific skills;
        ii. so called soft skills;
    b. project objectives.
4. Take it slow. The most important outcome is the quality of the experience for the participants, not the quantity of the output.
5. Always finish each workshop with a reflection on how the workshop went for each participant. See Guidelines for Workshop Reflection.

Zoom:

Account Settings - Meeting:

Security:

1. Require a password when scheduling new meetings: YES
2. Require a password for instant meetings: YES
3. Require password for participants joining by phone: YES

4. Waiting room: YES
    a. Choose which participants to place in the waiting room: EVERYONE
5. Embed password in invite link for one-click join: NO
    a. Users must type in their password
6. Only authenticated users can join meetings: NO
    a. It's not appropriate for us to require under-16's to have a Zoom account
7. Only authenticated users can join meetings from Web client: NO
    a. See above

Schedule Meeting:

8. Host video: YES
    a. So participants can confirm who you are straight away
9. Participants video: NO
    a. So participants can control their own visibility
10. Audio Type: TELEPHONE AND COMPUTER AUDIO
11. Join before host: NO
    a. The host and another member of Digital Writes staff, or volunteer, or other responsible adult must be in the meeting before it begins
12. Enable Personal Meeting ID: NO
    a. We prefer you to disable this so you don't accidentally start a meeting that doesn't meet the conditions in these guidelines;
    b. Remember, your personal meeting ID is essentially a personal phone number that people can "drop in" on at any time.
13. Mute participants upon entry: NO
    a. We're only working in small groups, so this shouldn't be necessary

In Meeting (Basic):

14. Require encryption for 3rd party endpoints (SIP/H.323): YES
15. Chat - Allow meeting participants to send a message visible to all participants: YES
    a. Prevent participants from saving chat: NO
16. Private chat - Allow meeting participants to send a private 1:1 message to another participant: NO
17. File transfer - Hosts and participants can send files through the in-meeting chat: NO
    a. This can be enabled during the meeting if needed
18. Feedback to Zoom: NO
19. Display end-of-meeting experience feedback survey: NO
    a. We have our own Guidelines for Workshop Reflection
20. Co-host - Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host: YES
    a. The second adult should co-host.
21. Polling - Add 'Polls' to the meeting controls. This allows the host to survey the attendees. YES
    a. So we can vote on ideas if necessary. Although general consensus through discussion is much more preferable.

22. Screen sharing - Allow host and participants to share their screen or content during meetings: YES
    a. Who can share? Host Only: YES
    b. So participants can't inadvertently put themselves at risk.
23. Disable desktop/screen share for users: NO
    a. This only applies to Users registered on our account. Since we don't have Users or use User Management, this won't apply.
24. Annotation - Allow host and participants to use annotation tools to add information to shared screens: YES
    a. Allow saving of shared screens with annotations: YES
25. Whiteboard - Allow host and participants to share whiteboard during a meeting: YES
    a. Allow saving of whiteboard content: YES
    b. Auto save whiteboard content when sharing is stopped: YES
26. Remote control - During screen sharing, the person who is sharing can allow others to control the shared content: NO
27. Nonverbal feedback - Participants in a meeting can provide nonverbal feedback and express opinions by clicking on icons in the Participants panel: YES
28. Allow removed participants to rejoin - Allows previously removed meeting participants and webinar panelists to rejoin: YES
    a. Our protocol (below) has you close off entry to the meeting once it starts. If you agree to allow a removed participant to rejoin, via email for example, you can open it up again for them.
29. Allow participants to rename themselves: YES
    a. This allows participants to have control over their privacy.
    b. If they use an offensive username, immediately remove them from the meeting.
30. Hide participant profile pictures in a meeting - All participant profile pictures will be hidden and only the names of participants will be displayed on the video screen. Participants will not be able to update their profile pictures in the meeting.
    a. This is to preserve participant's privacy.

In Meeting (Advanced):

31. ALL OFF, except:
32. Virtual background - Customize your background to keep your environment private from others in a meeting. This can be used with or without a green screen: YES
    a. This allows participants to have control over their privacy.
    b. Allow use of videos for virtual backgrounds: NO
        i. This would be too distracting.

Email Notification:

33. When a cloud recording is available - Notify host when cloud recording is available: YES
    a. Send a copy to the person who scheduled the meeting/webinar for the host: YES

34. When attendees join meeting before host: YES
    a. With the Settings above this should never happen. If it does, take this as a warning that you need to review your settings.
35. When a meeting is cancelled: YES
36. When an alternative host is set or removed from a meeting: YES
    a. This should never apply.
37. When someone scheduled a meeting for a host
    a. Since we don't have registered users this should never apply.
38. When the cloud recording is going to be permanently deleted from trash: YES

Other:

39. Blur snapshot on iOS task switcher: YES
    a. Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window.
40. Invitation Email: ENGLISH
41. Schedule Privilege: NONE

Account Settings - Recording:

1. Local recording: YES
    a. Hosts can give participants the permission to record locally: NO
    b. In line with our Safeguarding Policy we record all meetings.
2. Cloud recording. Check the following settings to ON:
    a. Record an audio only file.
    b. Save chat messages from the meeting / webinar.
    c. This is just as a backup for our local recordings, so we don't need video.
    d. Add a timestamp to the recording
    e. Display participants' names in the recording
3. Automatic recording
    a. Record on the local computer: YES
4. IP Address Access Control: NO
5. Only authenticated users can view cloud recordings: YES
6. Require password to access shared cloud recordings: YES
    a. Password protection will be enforced for shared cloud recordings. A random password will be generated which can be modified by the users. This setting is applicable for newly generated recordings only. This means only Digital Writes' staff will have access to cloud recordings.

Account Settings - Telephone:

1. Show international numbers link on the invitation email - NO
2. Choose where most of the participants call into or call from the meeting: EUROPE
3. 3rd Party Audio: OFF
4. Mask phone number in the participant list: YES
5. Global Dial-in Countries/Regions: UNITED KINGDOM

Zoom Meeting Protocol:

1. Schedule all meetings in advance. Do not use your personal ID.
2. Give the meeting a meaningful name, including possibly:
    a. Project title
    b. Group name
    c. Subject
    d. Date
3. Always require a password.
4. Send a meeting invitation to all participants to their school email account (or other approved email) from your secure Digital Writes email account.
5. Start the meeting and do the following preflight checks:
    a. Confirm that Host Video is on and Participants' Video is off.
    b. Confirm the following in Advanced Options:
        i. Waiting Room: ON
        ii. Enable join before host: OFF
        iii. Mute participants upon entry: OFF
        iv. Only authenticated users can join: OFF
        v. Automatically record meeting: ON
        vi. Check that the green shield with the tick is visible to confirm "You are using enhanced encryption"
        vii. Check that the meeting is recording
    c. Check Share Screen Options:
        i. Click on the little up-arrow by Share Screen
        ii. Click on Advanced Sharing Options
        iii. Confirm: Who can share: ONLY HOST
6. If a participant behaves inappropriately, you can either put them back into the Waiting Room for a time, or Remove them completely.
    a. Give them a warning;
    b. Put them in the waiting room for a fixed time
    c. If that doesn't work, Remove them from this session permanently
    d. Contact them via email to address the issue according to our Codes of Conduct and other policies.