Social Media & Digital Safety Policy

(December 2023)

DOCUMENT CONTROL	
Document name	Social Media and Digital Safety Policy
Document type	Policy and Procedures
Approved by and date of approval	Governing Board (16-12-2023)
Date it takes effect	20-12-2023
Date it will next be reviewed	20-12-2024
Related documents that should be read with this one	Safeguarding Policy, Positive Behaviour Policy (R-07), International Programme Guides, Programme Basic Rules (C-03), Policy and Procedure for Enforcement of Rules (R-11), Procedure for Sending Someone Home (R-15).
Name of the document this replaces	R-17A CISV International Social Media Guidelines
Document author	International Safeguarding and Risk Management Team

Contents

Introduction

Within CISV, social media, online platforms, and digital channels are essential components of our daily operations and interactions. They offer us powerful, enjoyable, and effective means to support CISV's mission and values.

While these online/digital spaces provide numerous benefits and opportunities, CISV acknowledges that they also pose various safeguarding risks, especially to CISV children and adults at risk. It is crucial that we comprehend and manage these online-associated risks to ensure the safety and well-being of all individuals involved in CISV.

This Social Media and Digital Safety Policy outlines CISV's steadfast commitment to safeguarding CISV children and adults in the online/digital space. We firmly believe that everyone in CISV has the right to safety, and this policy serves as the cornerstone of our efforts to achieve this goal.

This policy and procedures set forth the principles and guidelines that govern CISV employees and volunteers' interactions with children and adults in the online/digital space, regardless of the online platform or digital channel used. It provides instruction to CISV employees and volunteers on how to use social media and other digital/online spaces for official CISV use. It also outlines the expectations of CISV employees and volunteers regarding the appropriate and safe use of online/digital spaces for personal use. This policy and procedures apply to all CISV employees and volunteers in all CISV activities.

Social Media and Digital Safety Policy

Purpose and Scope:

CISV is committed to prioritising the safety and well-being of all members of the CISV community. In an increasingly online/digital world, it is our duty to ensure that everyone in CISV is safe when interacting with other members of the CISV community in the online/digital space. This Social Media and Digital Safety Policy outlines our dedication to creating a positive, inclusive, and safe online/digital environment across CISV.

The following rules apply to all CISV employees and volunteers, whether in local, national and/or international settings regarding interactions with and between CISV children, and CISV children and adults, using digital channels and online platforms for official and/or unofficial/personal CISV purposes.

This policy and procedures is not exhaustive; as the digital/online space rapidly evolves, CISV employees and volunteers need to consider changes in digital/online landscape and the full range of risks. The International Office endeavors to train and support volunteers and employees with this.

For wider members of the CISV community, such as parent(s)/guardian(s) interacting with CISV's social media accounts and people attending open days, refer to the CISV Social Media Community Guidelines.

Supporting Documents:

This policy and procedures must be considered in conjunction with several other CISV policies and procedures, including the CISV: Safeguarding Policy, Positive Behaviour Policy, and Data Protection Policy and Guidelines.

Additionally, it is essential to align this policy and procedures with pertinent local laws in the country where it is being applied. It should take precedence over local regulations if they are less stringent.

Policy Principles:

These principles serve as the cornerstone of our Social Media and Digital Safety Policy. We believe that:

- **Safety is Paramount:** The safety and wellbeing of everyone is our top priority, both in the physical and online worlds.
- **Best Interests of the Child:** In matters concerning children, the best interests of the child are paramount and should be the primary consideration.
- **Legal Compliance:** We will strictly adhere to international and local laws and regulations concerning safeguarding, online privacy, and data security. This includes adhering to The United Nations Convention on the Rights of the Child (UNCRC), GDPR, and relevant local and/or national laws.
- **Diversity and Inclusion:** We will prioritise the safety of every child and adult at risk, irrespective of their age, gender identity, abilities, ethnicity, race, sexual orientation, or socioeconomic background. Every individual has the right to receive equal protection from all forms of abuse and harm.
- **Stringent Data Protection:** We will rigorously adhere to the privacy of persons and their personal information. Data will only be collected and used for its intended purpose and will never be shared without consent unless there is a lawful reason to do so.
- **Informed Consent for Visual Media:** Appropriate informed consent will be obtained before collecting and using photos or videos of CISV children on official CISV platforms.
- **Safe Online Environments:** Official CISV platforms will maintain a safe and respectful environment, free from bullying, harassment and discrimination, or inappropriate content.
- **Continuous adaption:** We will proactively assess, monitor, and adapt our online safety practices to keep pace with evolving technologies and emerging threats, and implement learnings from safeguarding incidents.
- **Cultural Sensitivity and Recognition of Local Contexts:** Our Social Media and Digital Safety Policy will reflect and respect the diverse cultures, languages, and context in which we operate, ensuring a culturally sensitive and relevant approach. In cases of conflict between local customs and our values, we will prioritise the protections outlined in the Universal Declaration of Human Rights and the UNCRC.
- **Safety Overrides Data Protection:** If there are reasonable concerns for someone's safety, those concerns take precedence over data protection considerations. Information must be shared with relevant parties to ensure the person's safety, while every effort will be made to maintain confidentiality for all involved parties. Information will only be shared with those who need to know to address the concern.

Policy Monitoring and Review:

CISV International keeps a record of all incidents reported, inquiries made, and actions taken. We also summarize incidents anonymously and keep them in a database of issues.

Every year the International Office employees analyze all reported safeguarding issues for the organization to identify learning, development potential, and actions to be taken to improve CISV. This information then leads to any review or update of our policies and procedures if issues are identified.

CISV International's Risk Management and Safeguarding Committee will review this policy and its procedures every three years.

Terms and Definitions

- **Online harms**: anything online which causes a person distress or harm. This encompasses a huge amount of content and can be very subjective depending on who is doing the viewing; what may be harmful to one person might not be considered an issue by someone else[1]. For examples, click here.

- **Digital safeguarding:** involves protecting everyone from online harms. Click here for some examples.

- **Social media:** Social media are interactive technologies that facilitate the creation and sharing of content, ideas, interests, and other forms of expression through virtual communities and networks [1].

- **Digital/online space: '**Digital' refers to electronic technology, such as mobile phones, laptops, tablets, and smartwatches, that can make and store photos and videos. 'Online' refers to something that is connected to the internet. Therefore, the 'digital/online space' includes but is not limited to websites, social media platforms (e.g., Facebook, Instagram, and X (formally known as Twitter), SMS and instant messaging services (e.g., WhatsApp, Viber, Telegram, and Messenger), video conferencing tools (e.g., Zoom, Microsoft Teams, and FaceTime), and the use of digital photography, video, and live streaming.

- **Platform:** Any internet-based platform, including those which may be accessed through an app, through which users are able to create and/or share content[2].

- **Live streaming:** Live streaming technology lets you watch, create and share videos in real time[3].

- **Official CISV use**: any activities within the online/digital space undertaken by someone acting in their role as a CISV employee or volunteer and for the specific purpose of that role within CISV. Official accounts can use the CISV branding and therefore, are the intellectual property of CISV. These accounts should reflect CISV's policies, procedures, and values. An example of official CISV use or an official CISV account would be an Instagram page set up for a NA, Chapter or Junior Branch, run by volunteers of that NA, Chapter or Junior Branch to promote and support their organisation's work as a Member of CISV.

- **Unofficial CISV use:** unofficial CISV use includes any accounts or online spaces set up outside of the jurisdiction of CISV, or their NA, Chapter, or Junior Branch. These accounts or online spaces are considered "unofficial" and are created without specific authorisation or consent from CISV, or their NA, Chapter or Junior Branch. They are not operated, managed, or endorsed in an official capacity by CISV employees or volunteers as part of their role. Unofficial CISV groups cannot use our CISV branding such as our logo and must include a disclaimer within their page information or clearly state within the group that they are not affiliated with CISV. CISV cannot take action on these sorts of accounts.

Please refer to full list of safeguarding terms and definitions in 'Terms and Definitions' section of the CISV Safeguarding Policy.

[1] J. H. Kietzmann, K Hermkens, I. P. McCarthy, B. S. Silvestre, *'Social media? Get serious! Understanding the functional building blocks of social media'*, Business Horizons, Volume 54, Issue 3, 2011, https://doi.org/10.1016/j.bushor.2011.01.005
[2] www.lawinsider.com/dictionary/social-media-platform
[3] https://www.thinkuknow.co.uk/parents/articles/what-is-live-streaming/

Procedure 1: Choosing Digital/Online Platforms for Official CISV Use

The landscape of social media and digital/online platforms is constantly evolving. When deciding which platforms to use for official CISV purposes, CISV employees and volunteers must consider the following factors: the purpose, terms and conditions, benefits and safeguarding risks, and the law.

1. Purpose

When deciding how to share information, consider the context, intended audience and whether the platform is appropriate for the type of information/communication.

Critical programme information – email preferred:

For example, when communicating with parent(s)/guardian(s) programme itineraries, programme updates, and forms email is generally the best choice:

- It allows for sending longer, detailed messages, and secure attachments, which can be password protected/encrypted. For further advice on sharing information securely via email contact the International Office IT Support Officer at myCISV@Support.cisv.org.
- Email ensures delivery to individual recipients and creates a record of communication.

Non-critical information/business – social media and WhatsApp allowed:

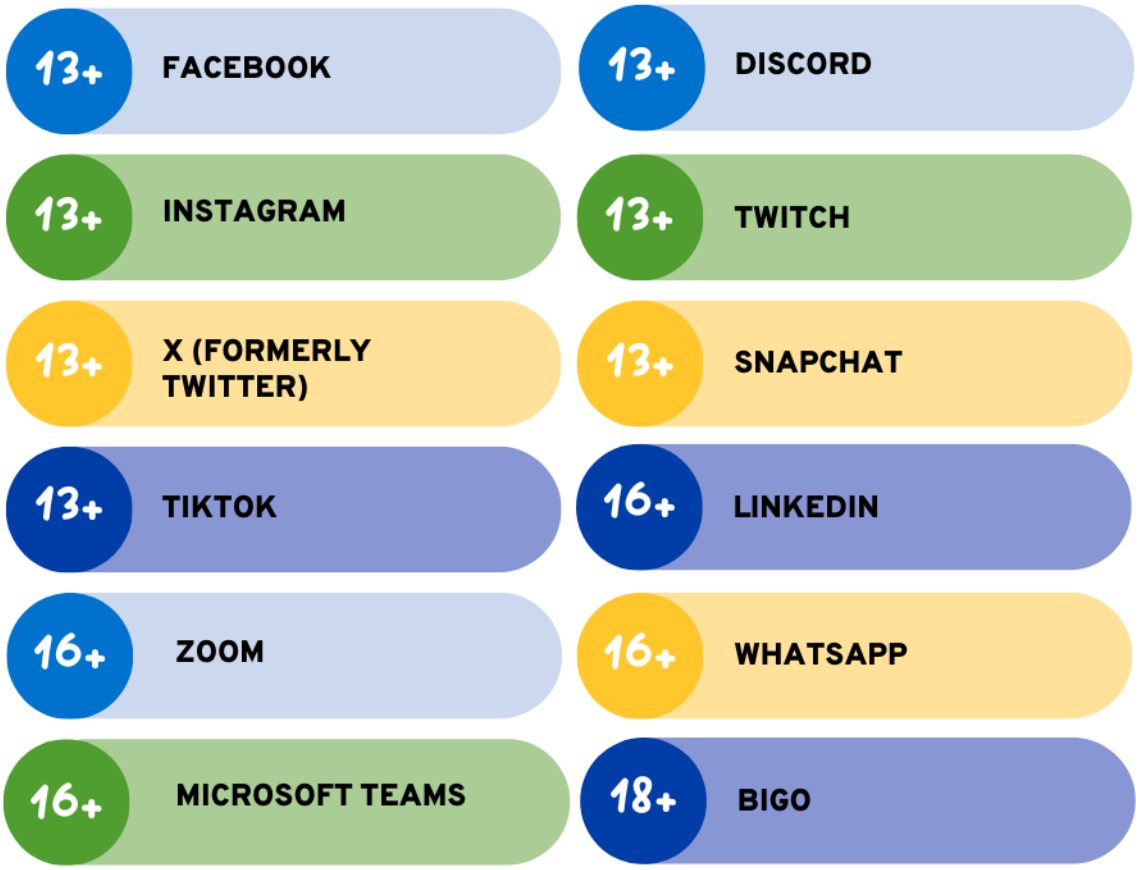
For example, when updating parent(s)/guardian(s), promoting a CISV activity, connecting with past participants, or sharing CISV's mission a more informal platform like WhatsApp may be useful:

- These tools enable quick updates on activities, photo sharing, and building a sense of community.
- However, confidential, and sensitive information must only be handled through GDPR compliant and secure online platforms.
- Formal processes should still be conducted through official channels.
- Staff should be cautious about the content they post on social media and other informal platforms, especially when sharing photos of participants.

2. Terms and Conditions

Details regarding the terms and conditions of a social media or digital platform, including age requirements, are typically available on the provider's website. You must consider the terms and conditions when selecting a platform for use.

Here are the age ratings for some poplar online platforms in 2023:



3. Benefits and Risks

Here are some examples of **online harms** that must be considered when thinking about potential online risks and how we protect everyone in CISV from them:

- **Sharing of harmful and extreme content online**: this includes the sharing or child sexual abuse material, as well as content that encourages violence, hate or terrorism online.
- **Sharing of inappropriate content online**: this involves sharing sexually explicit material or violent and offensive content online. It also includes children and young people sharing explicit images or videos of themselves or others.
- **Sharing personal identifiable information online**: this pertains to sharing information that makes the child identifiable, such as their full name or details related to their protected characteristic(s), such as their religion, ethnicity, or sexual orientation. It also includes revealing information that could be used to locate a child, like their current location during a CISV programme or their place of residence. Additionally, sharing information about a child's emotions or thoughts can be problematic, as this may be used for grooming.
- **Sexual exploitation and grooming online**: is a process that involves someone developing a relationship and trust with a child, and sometimes with their family, so that they can abuse them.

Grooming can happen in person and online. Click here for more information from the NSPCC about potential signs and actions to take if concerned about grooming.

- **Promoting self-harm, suicide and eating disorders online**: this includes online content encouraging harmful behaviours like self-harm, suicide or eating disorders.
- **Bullying online / Cyberbullying:** this encompasses offensive, intimidating, malicious, insulting behaviour, and abuse of power in online spaces.

The table below offers a summary of some current risks linked to specific digital/online platforms commonly used for official CISV purposes. This is not an exhaustive or recommended list:

Platform	Benefits	Risks
Facebook	• Social networking and connection • Sharing updates and photos • Joining groups and communities • Bans and removes harmful content	• Names and identities can be revealed through tagging in posts. • Option of live video streaming. • Option of tagging with the geo-location. • Direct messaging can facilitate unsupervised 1-1 communication.
WhatsApp	• Instant messaging • Voice and video calls • Group chats and file sharing	• Telephone numbers of members of a group can be visible to everyone else in the group. • No one from outside a group can monitor the communications. • People can be added to groups by people they don't know. • Option of disappearing messaging. • Option of live location sharing.
Instagram	• Visual storytelling • Photo and video sharing • Discovering trends and inspiration • Popular among a younger audience • Bans and removes harmful content	• Direct messaging can facilitate unsupervised 1-1 communication. • Option of disappearing messaging. • Option of tagging with the geo-location.
Microsoft Teams	• Uses strong encryption protocols • Collaborative workspace • Real-time chat and video conferencing	• Meetings can be joined without login details if organisers allow.
Snapchat	• Chatting with friends in real-time • The content length for Snapchat is quite short, making it fun to make content. • Snapchat is very creative and engaging especially for a younger audience.	• Disappearing messaging meaning you can lose a message trail/evidence. • Children can share their infomation with strangers and be quickly located. Snapchat settings can put people in danger by allowing anyone to follow their account.

Procedure 2: Running Official CISV Social Media Accounts

1. Authorisation, Permission and Access Rights

i. To create new official CISV accounts you need prior approval from the respective board members of the Chapter, National Association or Junior Branch.
ii. All Chapter, National Association, and Junior Branch boards must approve the appointment of two account administrators/moderators as described in section 2 (below). Administrators/Moderators. For a Pilot Role Profile click here.
iii. These boards must also maintain a record of all their official CISV accounts, the respective account administrators/moderators, and account login details (usernames and passwords).

2. Administrators/Moderators

i. For all official CISV Chapter, National Association, and Junior Branch social media accounts, a minimum of two CISV volunteers must oversee and supervise the operation, including all activity and content, of each account and serve as administrators/moderators. All activity and content include but are not limited to moderating: comments, photos, videos, and posts, and private messages to official accounts.
ii. The administrators/moderators must be at least 16 years of age, and one of them must be at least 18 years of age. If one administrator/moderator is aged 16 or 17 years old, they must be supervised and supported by the other, adult administrator/moderator. Their ages must align with the platform's terms and conditions and relevant local laws.
iii. The administrators/moderators must be registered on MyCISV in the role of 'Social Media Administrator/Moderator'.
iv. The administrators/moderators must have completed the required safeguarding training requirements (see the CISV Safeguarding Policy) and be confident with safeguarding requirements in the digital/online world.
v. If necessary, this responsibility/role can be in addition to another role and/or pre-existing role that the volunteer holds, so long as there is always at least two people and the responsibilities are fulfilled.
vi. When an official administrator/moderator steps down or leaves CISV, they must not access the account and the account's username and password must be changed by the newly appointed administrator/moderator.

3. Safety Measures

i. **Privacy settings:** All official CISV accounts must use suitable privacy settings and disable geo-tagging where possible.

ii. **Passwords:** Password protection with a strong, unique password is mandatory for all official CISV accounts, and it's recommended to consider security answers.
iii. **Verify friends/users:** For any official CISV forums or official CISV online groups where users need to request to join a group such as on Facebook, account administrators/moderators must verify friend/user requests, and block unknown individuals, fake accounts, or suspicious profiles. This does not apply to followers.
iv. **Moderate content:** Account administrators/moderators must use relevant settings/tools to moderate others' content and activities, including reviewing content before it's published and managing who can comment.
v. **Reporting mechanisms:** All official CISV accounts must incorporate a clear reporting mechanism. Many online/digital platforms have built-in reporting systems that directly reach platform administrators. Additionally, there must be a clear method to report concerns directly to the account administrators/moderators. Any safeguarding concerns identified or reported through CISV digital/online platforms must be handled in the same way as in the physical world, following the CISV Safeguarding Policy Procedure 5: Safeguarding Incidents.

4. Content and Activity

i. **Promoting our mission:** CISV's use of social media platforms is intended to promote and support the organisation's mission. Therefore, any content shared should directly relate to and reinforce the principles of peace, diversity, and cross-cultural understanding. Messages should aim to inspire, educate, and engage the global community in activities that further our objectives.
ii. **Promoting tolerance and understanding:** Our social media platforms should serve as beacons of tolerance, empathy, and understanding. Messages should be framed in a way that fosters dialogue and cooperation, rather than division or confrontation. Content should not promote or highlight one side of a conflict over another. Volunteers should exercise sensitivity when discussing contentious issues and prioritise messages that encourage peaceful resolutions and dialogue.
iii. **Non-religious, Non-Political and Non-Governmental Content:** CISV was founded as an inclusive, non-political, non-governmental organisation. Administrators/moderators of all official CISV accounts should refrain from sharing or endorsing content or activity that advocates for or against any political party, government, religion, or faith. We acknowledge the complexity of this, and there is a great deal of nuance on this topic. If you have any concerns about any content, please contact our International Communications Team.
iv. **Inflammatory or controversial content:** Content that may provoke strong emotions or conflict, such as unnecessary inflammatory or controversial topics, should be avoided.
v. **Alcohol and tobacco:** There must be no content which shows, or is indicative of, the consumption of tobacco or alcohol in CISV activities involving children.
vi. **Clear branding:** Official CISV accounts must prominently state in writing that they are an *'official CISV account'* and specify their affiliation with a National Association, Chapter, Junior Branch, or the International Office. Usage of the official CISV branding is mandatory for all official CISV accounts, requiring full authorisation as outlined in B) Authorisation, Permission and Access Rights.
vii. **Consistent Identity:** All official CISV accounts must maintain a consistent visual identity, following CISV's "Looking Good" Brand Guidelines. For further guidance contact CISV International Communications Officer.

viii. **Compliance:** Content and activity must adhere to the laws of the respective country/countries, as well as the terms and conditions and guidelines set by each individual platform.
ix. **Removing content:** Account Administrators/Moderators must promptly remove/hide any content or activity that violates the platform's terms and conditions and/or this policy and procedures.
x. **Reporting:** Any content that violates the platform's terms and conditions must be reported to the platform. Any content or activity contravening this policy must be reported to the International Communications Officer. Safeguarding concerns (recent and noon-recent) must be handled in the same way as in the physical world, following CISV Safeguarding Policy Procedure 5: Safeguarding Incidents.
xi. The procedures on Digital Communication and Digital Photography, Video and Live Streaming must be followed for all content and activity.

If you are unsure, please reach out to the CISV International Communications Officer and the Risk Management and Safeguarding Team for guidance and support.

Procedure 3: Digital Communication

Digital communication encompasses various methods, including but not limited to emailing, texting, video calling and instant messaging. We need to ensure that there are clear and well-defined limits and guidelines around digital communication between CISV children and CISV employees and volunteers. These boundaries serve as a protective framework to create a safe environment for both the children and the volunteers and employees themselves.

1. Adding or Following CISV Children

i. Do not add/follow individual or groups of CISV children on any personal online platform.
ii. If a child or adult joins CISV and they already have a connection on an online platform, it is the responsibility of the adult to adhere to and communicate the boundaries of the online contact in accordance with our policies and procedures.
iii. Exceptions can be made if you have a preexisting relationship with a CISV child outside of CISV, such as being a family member or close family friend. In such cases, inform the parent/guardian of the online connection.

2. Private Online Communication

i. Adults should not engage in 1-1 private online communication with an individual or group of CISV children.
ii. If a CISV child contacts you individually online, acknowledge their message and sensitively explain that private contact is not permitted between CISV children and CISV adult employees/volunteers.
iii. Exceptions can be made in specific situations:
   - Where a child is in an official CISV role such as a Board Member or Committee member, and the communication with another Board or Committee member, and the nature of the communication is official and instructional.
   - Where a child is at risk of harm and the communications relates to a child's safety, in which case it may be more important to engage and respond to the communication, following the CISV Safeguarding Policy Procedure 5 Safeguarding Incidents.
   - Where the communication is from an adult in a position of trust and responsibility to a member of Junior Branch/Junior Counsellor about their role/responsibilities, and the nature of the communication is official and instructional.

3. Group Online Engagement for Official CISV Use

i. When engaging groups of CISV children on online/digital platforms for official CISV purposes, ensure a clear purpose, such as Leaders preparing their delegation for a programme and setting up meeting times.
ii. Communicate the group's purpose to the parent(s)/guardian(s), the Risk Manager, and all members.

iii. Always have *at least* two CISV adults in positions of trust and responsibility in the group. Having two adults within the group provides important accountability, oversight, and protection for both the adults and the children.
iv. Verify who has access and ensure that it is limited to those who should have access.

4. Compliance with Platform Terms and Conditions

i. Any online communications with groups of CISV children for official CISV use must comply with the platform's terms and conditions and applicable laws.

5. Post-CISV Activity Contact

i. Online/digital communication with groups of CISV children should finish after the CISV activity has ended, or soon thereafter. If you need to continue any online contact in an official CISV capacity with groups of CISV children for legitimate interests (e.g., debrief and closure-type activities, reunions, collecting feedback, promoting activities/opportunities) you must obtain confirmation and consent using the Communications and Publicity Consent section of the existing Legal Form (*coming soon in 2024*) . You must also communicate the purpose and timeframe of this ongoing contact with your Risk Manager or Chapter Board, and the parent(s)/guardian(s).

6. Protection of Personal Information

i. Never disclose or share personal identifiable information about CISV children on personal or official CISV social media platforms.
ii. Do not share information that reveals the location of a child in CISV activities, such as posting the camp's address before or during the programme, unless this is on a need-to-know basis and via a secure platform.
iii. Consider whether any personal devices, such as smart watches, could share the location of a CISV activity involving children publicly, and ensure that settings are checked and, if necessary, changed to mitigate against this.

7. Appropriate Language

i. Use language that is respectful and appropriate. Never use language that could be considered discriminatory, derogatory, threatening, abusive or sexualized.

8. Video Calls

i. When conducting video calls for official CISV use during a CISV activity involving children, ensure it takes place in a neutral area with nothing that could identify a child or be perceived as inappropriate in the background.

ii. Do not record video calls unless it is for a legitimate reason, such as an internal fact-finding enquiry, and all participants are aware of and have verbally consented to the recording before it has started and have had the opportunity to opt-out or turn off their video. Ensure that recordings are deleted once there is no longer a legitimate purpose for them.

CISV employees and volunteers must report *all* safeguarding concerns in CISV activity, offline or online, following the CISV Safeguarding Policy Procedure 5: Safeguarding Incidents. If you are unsure, please reach out to the CISV International Communications Officer and the Risk Management and Safeguarding Team for guidance and support.

Procedure 4: Digital Photography, Video, and Live Streaming

CISV values the positive and educational experiences of CISV children, which can be shared with parents/guardians and the wider CISV community through photography and video. However, the use of photos/video on official CISV online platforms must be managed carefully to avoid safeguarding risks to CISV children. Some individuals may also have concerns about their images or videos being taken, stored, and used by CISV.

1. Informed Consent

i. **Written Consent:** You must obtain written consent, using the Communications and Publicity Consent section of the existing Legal Form (*coming soon in 2024*), from the child's parents/guardians, and from the young person if over 16 years old. This should be done before any CISV activity that involves children begins. Note that the requirement to have written consent does not apply to children taking photos/videos of each other. You can translate and digitalise the form as long as the content stays true and corresponds to the content and format, to ensure consistency across the organisation.

ii. **Verbal Consent:** In addition to written consent, you must also obtain verbal consent from the child before taking any photo/video. Always respect their wishes and feelings before, during, and after taking the photographs/video, and sharing them. With adults, consider people's privacy, consider if the person would be comfortable with their image/video being taken and if in doubt, ask them as per our Social Media Community Guidelines.

2. Taking Photographs and Videos

i. **Volunteer Designated Photographers/Videographers:** Each CISV activity that involves children must designate a limited number of persons to take photos/videos at a CISV activity involving children. This must be existing CISV volunteers in positions of trust and responsibility. No other CISV volunteers or employees should take photos/videos of CISV children (identifiable or not). These designated persons must have access to all the delegates' Legal Forms, which contains a section on Communications and Publicity Consent, and a clear understanding of who has consented and who hasn't before the CISV activity.

ii. **Designated device**: It is recommended that the Designated Photographers/Videographers (*see above*) use a Chapter/National Association/Junior Branch-owned device for their role, rather than using a personal device. This is a precautionary recommendation that helps to protect children and volunteers.

iii. **Clothing:** The Designated Photographer/Videographer (*see 2.i above*) must ensure that children are appropriately clothed, so that parts of the body which are private, and which are not usually visible in public settings are covered.
iv. **Swimming/Water Activities:** The Designated Photographer/Videographer (*see 2.i above*) must not take photos/film of children during swimming/water activities when they are visible in their swimwear.
v. **Sensible Camera Angles:** The Designated Photographer/Videographer (*see 2.i above*) should avoid camera angles that could be misinterpreted or misused by others, for example, angles which focus on private areas of the child's body.
vi. **Focus on Activities/Groups:** We recommend that when the Designated Photographer/Videographer (*see 2.i above*) is photographing/videoing children, the focus is on a group context and activities with multiple children, and consent has been obtained for all visible children.
vii. **Social Media Sharing:** Never share a photograph/video of a CISV child or children on your personal social media account(s), except when sharing CISV Chapter or National Association promotional posts from an official CISV account on your personal social media to promote CISV activities.
viii. **Prohibited Areas:** All photography, video recording, and livestreaming are strictly prohibited in areas such as changing rooms, toilets, showers, and first-aid/medical rooms.
ix. **Background Considerations:** When the Designated Photographer/Videographer (*see 2.i above*) is capturing photographs or videos, make sure that there is nothing identifiable or inappropriate in the background that may be heard or seen.

3. Sharing Photographs and Videos

i. **Tagging:** Never tag a child or CISV person in a photograph or video.
ii. **Privacy:** Do not share or reveal the full name of a child in a photograph/video on social media.
iii. **Location Details:** Refrain from sharing the current location of CISV activity involving children through images/videos that show street names, names of sites or identifiable buildings.
iv. **Group Sharing:** After a CISV activity involving children, sharing of images, photographs and videos taken during these activities must only occur directly with the participants as a full group. The parents/guardians of the children must be included as outlined in the Digital communication section. The image-sharing platform must be secure, allowing access only to those authorised and verified, such as the parent(s)/guardian(s) of the children. For advice on using MyCISV to securely share material from a CISV activity contact the International Office IT Support Officer at myCISV@Support.cisv.org.
v. **Awareness:** Everyone with access to images from a CISV activity involving children must be reminded of the rules regarding the sharing of CISV images/video.
vi. **Permissions from Other Organisations:** When collaborating with other organizations alongside CISV, ensure that you obtain proper written permission to use any photographs, videos etc. that include children from the other organizations and vice versa.

4. Storing Photographs and Videos

i. **Legitimate Interests:** There must be a legitimate interest or use for marketing or communications purpose for storing photographs/videos after an event has ended.
ii. **Labelling:** When securely storing photos, ensure they are labelled using the first name, camp name and year attended. This is to ensure that they can be tracked and deleted upon request.
iii. **Security:** Ensure that photos and videos are securely stored**.** Once stored securely, all photos/videos must be deleted from personal devices.
iv. **Consent:** Ensure that you are only storing material for which you have prior written consent in the Communications and Publicity Consent section of the Legal form. It is advisable that the material is stored alongside the respective communications and publicity consent form for that material, so that it is easy to track.
v. **Removal:** If there is a request to remove the content, you must be able to track the content and delete from all databases.

If you are unsure, please reach out to the CISV International Communications Officer and the Risk Management and Safeguarding Team for guidance and support.

Procedure 5: Responding to a CISV Safeguarding Incident Online

As a CISV employee or volunteer, there are several ways you might become aware of a CISV safeguarding incident online. These include but are not limited to:

- **Received Messages or Posts:** You receive or see a message or post from someone in CISV which makes you worried about their safety or wellbeing.
- **In-Person Disclosure:** When a CISV child discloses in-person that they are worried about someone in CISV taking, possessing and/or sharing inappropriate and/or indecent images/videos of them.
- **In-Person Disclosure (Bullying/Threats):** If a CISV child shares in-person that they are being bullied or receiving threatening or inappropriate messages online from someone in CISV.
- **Breach of Policy:** When you come across a post on an official CISV account or a CISV employee/volunteer's personal account, that violates this policy and procedures.

i. If you think that someone's safety is at immediate risk, you must take immediate protective actions to keep them safe, as outlined in CISV Safeguarding Policy Procedure 5 Safeguarding Incidents, 2. Responding.
ii. *All* safeguarding concerns (recent and non-recent) should be reported and recorded following the procedures outlined in CISV Safeguarding Policy Procedure 5 Safeguarding Incidents.

Appendix

Useful links:

- www.nspcc.org.uk/keeping-children-safe/online-safety/#guides
- www.thinkuknow.co.uk
- www.gov.uk/government/publications/charities-and-social-media
- glitchcharity.co.uk