UNIVERSITY OF WISCONSIN SYSTEM

Office of Compliance and Integrity
Katie Ignatowski | 608-265-2273 | kignatowski@uwsa.edu
Director of Compliance
1840 Van Hise Hall, 1220 Linden Drive, Madison, WI 53706
www.wisconsin.edu

TO: UW System Institution Precollege Liaisons

Guidance for Transitioning Precollege and Youth Activities to Virtual Platforms

Conduct and Interactions

1. Avoid one-on-one contact between adults and minors in video conferencing or email, text, chat, and other online communications.
    a. Programs should have at least two staff always present. If not possible, sessions should be recorded. (See recording guidelines below). Staff should never be one on one with a participant.
    b. All written correspondence should be sent from official program-issued devices and accounts and include program directors and parents or guardians.
    c. If responding to an individual email from a participant, include program directors and parents or guardians on response.
    d. If a participant reaches out via a method other than email, request that the participant send the question via email and cc parents or guardians.
    e. For virtual sessions, consider small group sessions instead of one-on-one sessions.
    f. Do not lead or participate in online video or audio sessions in public areas where strangers may be present. Never use a public kiosk or shared computer to access online learning video or audio sessions.
    g. Save email, chat, and text strings.
2. Communicate through official channels only. Do not interact with program participants through personal accounts on social media platforms like Facebook, Instagram, Twitter, Snapchat, and others.
    a. Youth participants may follow the program's social media accounts.
    b. Program staff may communicate with youth participants through the program's social media accounts. Avoid one-on-one interactions through direct messaging.
    c. If program participants request to friend or follow a program staff person's personal accounts, the program staff person must deny the request and report it to the program director.
    d. Social media accounts administered by the program should be reviewed daily for posts and comments which do not comply with policies or which may otherwise be considered offensive or inappropriate. Inappropriate comments, posts, videos, and pictures must be removed as soon as possible and reported to appropriate administrators for further potential action.
    e. If shared UW accounts on social media platforms are used, there should be some record of who has administrative access to those accounts. Passwords for those accounts should be recorded and securely stored, so that they can be accessed by Information security or other administrators, if necessary, in the case of an incident investigation.
    f. Passwords for UW institution social media accounts should comply with the password rules in UW System Administrative Policy 1030 Information Security: Authentication and UW System Administrative Policy 1030.A Information Security: Authentication Procedure
3. Limit interaction with program participants through video conferencing, email, and messaging between program staff and participants to reasonable program hours.

4. Participants must close all video conference applications at the end of each session to ensure that no inadvertent streaming of audio and/or video content unrelated to youth program activities occurs.
5. Do not use cell phones, cameras, imaging, or digital devices in an inappropriate way.
6. Ensure that background views in teleconferences follow the same guidelines that are used in physical office settings.
7. Do not make sexual or pornographic materials in any form available to minors or assist them in any way in gaining access to such materials. Do not use or be under the influence of alcohol or drugs during online interactions with minors.
8. Do not engage in discrimination or harassment. The University of Wisconsin System does not tolerate discrimination, discriminatory harassment, or retaliation in any form. (See Regent Policy Document 14-2: Sexual Violence and Sexual Harassment Policy)
9. Do not engage in verbal abuse toward or in the presence of a minor. Verbal abuse is defined as "harsh and insulting language direct at a person." (Merriam-Webster's Unabridged Dictionary)

Technology

1. Make online interactions visible, observable, and interruptible.
    a. Where possible, include more than one program staff member in program sessions.
    b. Consider recording the session.
        i. Consent to record must be obtained from parents in advance. *(See Attachment: Agreement for Assumption of Risk, Indemnification, Release, Precollege and Youth Virtual/Remote Programs form)*
        ii. Not all virtual meeting platforms have the capability to record sessions. Verify capabilities in advance.
        iii. Recordings should be created, stored, accessed and managed in a manner consistent with UW System Administrative Policy 1031 Information Security: Data Classification and Protection. Recordings should be stored centrally on the cloud using approved methods, never locally or on portable media such as USB or flash drives. Classes involving matriculated students may also be protected by FERPA.
        iv. Note that programs are for official use only and personal use or references is prohibited.
    c. Share the program schedule with parents or guardians and youth participants. Identify group activities, special events, and scheduled times for online tutoring or small group sessions. Encourage parents to help monitor their child's participation.
    d. Disable Private Chat or make all chats visible to the host (instructor or additional program staff) and save the chat transcript.
    e. Invite the program director to all meetings. Program Directors should drop into meetings often.
    f. Provide a way for the instructor or other staff to summon the Program Director to an online session.
    g. Provide a way for participants to offer feedback about their experience in the group.
2. Control access to the virtual platform.
    a. To invite participants to an online session, use blind copy (Bcc) to avoid cross-sharing everyone's email addresses. Copy the program director or a second staff member in the invitation.

b. The instructor should have and use a class roster, including verified email addresses and phone numbers, so participants can be identified by the instructors.
c. In a virtual setting, an image of a student along with their first and last name is considered personal identifiable information. In order to reduce the risk of exposure of the personal identifiable information of minors, programs are encouraged to have students to use only first name and last initial to identify themselves on platforms. Programs may also allow students to select alternative screen names, but must collect the alternative screen names during registration, so those names can be part of the student registration information on record. Note: If programs allow for alternative screen names, program staff must be able to verify unknown screen names through access to the participant roster/registration information.
d. Use the platform's "waiting room" feature and use the registration information on the program roster to verify identities before admitting devices to the session.
e. Take verbal attendance. Participants may join late due to technological issues.
f. Remove people whose identities cannot be verified. Attempt to verify identities verbally, through chat, and by comparing listed phone number against registration forms. Address any unauthorized participants present in remote locations (note that parents are an exception.)
g. Consider disabling software features which automatically save and enter user credentials, such as usernames and passwords, on all applications used in the youth learning program, including teleconferencing, in order to avoid unauthorized users from logging on and impersonating a youth program leader.
h. Set up sessions with one-time identifiers, not "personal rooms."
i. Password-protect sessions and send the password directly to rostered class members. Don't post it to a location visible to all participants or share links to teleconferences or classrooms via social media posts.
j. Disable participant screen sharing and file sharing, unless it is essential to the effectiveness of the activity.
k. Private or confidential information should never be shared in a group teleconference, by either program administrators or student participants.
l. Be sure to use the latest version of the virtual platform with the most recent patches of software wherever possible.

3. Use only devices and software approved by your institution and UW System.
    a. Consult with your institution's information security office to best understand risks and exposures.
    b. Review Pros and Cons of Virtual Platforms: Safety Considerations provided by the American Camp Association.
    c. Make sure you understand all capabilities of the platform you are using. Consult tutorials in advance of using a specific platform.
4. Post a privacy policy that complies with the Federal Trade Commission Children's Online Privacy Protection Act (COPPA) Guidance

Reporting Concerns

1. Follow your institution's incident reporting requirements to report online behavioral issues, suspicion of child abuse or neglect, and violations of campus policies.
2. If you notice any aberrant behavior of the computer used for the online session, you should contact the Help Desk immediately to report concerns. For example, the machine may have spyware on it that allows someone to remotely view the screen, including the teleconference.
3. Make sure participants know how to report problematic behavior, including threatening or inappropriate messages, cyberbullying, discrimination, harassment, sexual harassment, sexual assault or other behavior that violates law or policy. Each participant should be provided with contact information for the institution's Title IX Coordinator. (See Title IX of the Education Amendments of 1972, 20 U.S.C. § 1681 et seq., and Regent Policy Document 14-2: Sexual Violence and Sexual Harassment Policy)
4. Ensure all program staff (employees and LTEs) and volunteers have knowledge of the Title IX policies, including how to report concerns, as well as contact information for the institution's Title IX Coordinator.
5. Abide by all campus training mandates regarding mandated reporting, Title IX Responsible Employees and Clery Act.

Human Resources

1. All hiring requirements relating to working with minors continue to apply in a virtual setting, including but not limited to criminal background checks and Sex Offender Registry clearance.
    a. NOTE: Due to Covid-19 many backgrounds are either unable to be performed or significantly delayed. Best practices would be to hire staff who have been previously vetted by the institution as required by Regent Policy Document 20-19: University of Wisconsin System Criminal Background Check Policy and any other institution policies.

Indemnifications and Permissions

1. Programs must notify parents of all risks pertaining to the program. Parents must consent in writing to youth participating in virtual activity. Programs should disclose in the attached indemnification form the nature of all activities that will take place and any risks involved. Please consult with your university risk management office and refer to attached *Agreement for Assumption of Risk, Indemnification, Release, Precollege and Youth Virtual/Remote Programs form*.
    a. Note: Be sure to collect permission for each program or activity that a youth will participate in.

Funding and Cost Considerations

1. Please consult with state, federal, or other funding agencies if your program involves outside funding, such as DPI scholarships, in order to ensure that the activity meets agency requirements prior to the start of the program and reduce the risk of moneys not being allocated.
2. Be mindful of adjustments to program costs and fees that might be appropriate. Virtual programs may not involve the same amount of resources, and costs and fees should be adjusted accordingly wherever possible.

Recommendations

1. Please consult with your institution's Information Security, Risk Management, Human Resources, ADA/Disabilities, Legal (or UW System Office of General Counsel), and Compliance when creating a plan to transition precollege and youth activities to a virtual environment.

2. Programs should continue to abide by all applicable laws, policies and compliance standards in a virtual environment, including program quality review and Codes of Conduct. *(See Attachment: Sample Program Expectations and Parental Permission Form)*
3. For further guidance on virtual programming, see Best Practices for Keeping Your Online/Virtual Programming Safe for Campers provided by the American Camp Association.

Related Laws and Policies for Reference

1. Regent Policy Document 14-2: Sexual Violence and Sexual Harassment Policy https://www.wisconsin.edu/regents/policies/sexual-violence-and-sexual-harassment/
2. Regent Policy Document 14-6 Discrimination, Harassment, and Retaliation https://www.wisconsin.edu/regents/policies/discrimination-harassment-and-retaliation/
3. Regent Policy Document 20-19: University of Wisconsin System Criminal Background Check Policy Regent Policy Document 20-19: University of Wisconsin System Criminal Background Check Policy
4. Regent Policy Document 25-3 Acceptable Use Policy https://www.wisconsin.edu/regents/policies/acceptable-use-of-information-technology-resources/
5. Title IX of the Education Amendments of 1972, 20 U.S.C. § 1681 et seq., prohibits discrimination on the basis of sex in any educational program or activity receiving federal financial assistance. The University of Wisconsin System prohibits the following conduct: sexual discrimination, sexual harassment, sexual assault, dating violence, domestic violence, and stalking. https://www.justice.gov/crt/title-ix-education-amendments-1972; RPD 14-2 (see citation #1)
6. UW System Administrative Policy 1030 Information Security: Authentication https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/
7. UW System Administrative Policy 1030.A Information Security: Authentication Procedure https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/
8. UW System Administrative Policy 1031 Information Security: Data Classification and Protection https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/
9. UW System Administrative Policy 1032 Information Security: Awareness https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/
10. UW System Administrative Policy 1033 Information Security: Incident Response https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-incident-response/

Attachments

1. Sample Program Expectations and Parental Permission Form. **NOTE: this document needs to be updated with institution specific reporting information.**
2. Agreement for Assumption of Risk, Indemnification, Release, Precollege and Youth Virtual/Remote Programs Form. **NOTE: this document contains modifications to the standard UW System Assumption of Risk Form to suit precollege programs in a virtual environment. Check with your institution's Risk Management Office prior to utilizing this form.**

Sample Program Expectations and Parental Permission

Program/Activity/Camp Name: _____

Participant Name: _____

Parent/Guardian Name: _____

The Program has established standards of conduct for all Participants. It is the responsibility of the Parent/Legal Guardian and the Participant to review the Program rules and standards of conduct. Dismissed Participants may not be eligible for a refund of any fees or expenses.

The Program agrees to:

- Provide an agenda outlining the activities of the Program including the times, days, and how to access content.
- Collect registration information such as participant name, address, phone number, parents/guardian(s) name(s), phone number(s) and email(s).
- Provide a supply list and recommendations for setting up the home workspace to help participants fully engage in the program.
- Take attendance and only allow registered participants to participate.
- Only communicate with participants through official Program platforms.
- Ensure that two or more Program staff are present for the duration of the program.
- Keep conversations and interactions focused on the Program goals and objectives.
- Create an environment where everyone is welcomed and given the opportunity to succeed.
- Ensure that all participants are treated with dignity, fairness and respect. Harassment will not be tolerated. Hazing of any kind is prohibited. Cyberbullying is prohibited.
- Address problems that are brought to their attention.
- Will not share personal information, email, or social media accounts with minor participants.

The Participant agrees to:

- Participate in the digital environment to the same standard as a physical environment, including participating when called on, listening attentively, and minimizing distractions to others.
- Not share links or passwords for Program meetings or content.
- Challenge themselves to engage, be present and learn.
- Complete assigned projects on time.
- Request help if needed.
- Mute when not talking.
- Dress appropriately when on video.
- Not take inappropriate screenshots or images.
- Assume good intentions and have fun!

The Parent/Legal Guardian(s) agrees to:

- Assist the participant in setting up the home environment to meet the goals of the Program.
- Ensure the participant logs in on time and is prepared for the Program.
- Limit distractions and keep the participant safe throughout the duration of the Program.
- Allow time for the participant to complete required assignments.
- Communicate with staff prior to Program start time if the participant must be absent.
- Work with Program staff to resolve issues that may arise.
- Report illegal or inappropriate online behavior by staff or program participants [insert contact information for reporting concerns to the institution]

The following may result in being dismissed from the program:

- Bullying, harassing or using derogatory language towards another person or group of people.
- Being under the influence of alcohol or drugs.
- Repeated absences or failure to meet agreed upon program work requirements.
- Violation of a University code, policy, or regulation.

What are the consequences if the participant does not meet Program expectations?

- Staff will give a verbal or written warning regarding behaviors and actions that are not allowed and, in most cases, give the participant an opportunity to correct the behavior.
- Depending on the behavior, they may also contact the parent or legal guardian.
- In some cases, staff may require a corrective action plan in order to stay in the program.
- Some behaviors may result in immediate suspension or termination.

PARTICIPANT AGREEMENT

I understand that I must abide by the Program's expectations.

Participant Signature: _____ Date:_____

PARENT/LEGAL GUARDIAN AGREEMENT

I understand that my child and I must abide by the Program expectations. I understand that Dismissed Participants may not be eligible for a refund of any fees or expenses.

Parent/Guardian Signature: _____ Date: _____

Parent/Guardian Name: _____Date:_____

Agreement for Assumption of Risk, Indemnification, Release,
Precollege and Youth Virtual/Remote Programs

I desire to allow my minor child/ward to participate voluntarily in (insert name of program) at the University of Wisconsin- [insert name of institution] on (list program date). I UNDERSTAND THAT I AM BEING ASKED TO READ EACH OF THE FOLLOWING PARAGRAPHS CAREFULLY. I UNDERSTAND THAT IF I WISH TO DISCUSS ANY OF THE TERMS CONTAINED IN THIS AGREEMENT, I MAY CONTACT THE [list program contact name and phone number].

Assumption of Risks:
I understand that the [insert name of program], by its very nature, includes certain inherent risks that cannot be eliminated regardless of the care taken to avoid injuries. Some of these involve accidents and injuries, damages to property, the risk of data mining, phishing, viruses, malware, data breach of online information, cyberbullying, and other cyber risks. I understand that I have been advised to have health and accident insurance in effect for my child/ward along with appropriate property insurance coverage and that no such coverage is provided by the University or the State of Wisconsin. **I know, understand, and appreciate the risks that are inherent in the above-listed programs and activities. I hereby assert that my child/ward's participation is voluntary and that I knowingly assume all such risks.**

Hold Harmless, Indemnity and Release:
In consideration of permission for my child/ward to voluntarily participate in [insert name of program], today and on all future dates, I, for myself, my heirs, personal representatives or assigns, agree to defend, hold harmless, indemnify and release the Board of Regents of the University of Wisconsin System, the [name of institution] and their officers, employees, agents, and volunteers, from and against any and all claims, demands, actions, or causes of action of any sort on account of damage to personal property, or personal injury, or death which may result from my child/ward's participation in the above-listed program. This release includes claims based on the negligence of the Board of Regents of the University of Wisconsin System, the [name of institution] and their officers, employees, agents, and volunteers, but expressly does not include claims based on their intentional misconduct or gross negligence. **I understand that by agreeing to this clause I am releasing claims and giving up substantial rights, including my right to sue.**

Program Consent:
I hereby give permission for the [name of institution] to collect information from me and my child through an online platform, for the limited purpose of Program registration and participation. I understand that this information will not be shared with any third-party, unless otherwise required by the third-party platform provider for participation. I understand that all programs are subject to all [name of institution] guidance and policy around interacting in virtual spaces. For additional information on the University's privacy policies, please visit: [insert links to guidance and policies].

I further hereby authorize the [name of institution] to photograph and video/audio record my child during the Program, and use or distribute any photograph, audio or video recording ("Materials") related to Program activities that my child is depicted in. I also authorize use of these Materials for publication in a brochure, on [name of institution] websites, or other [name of institution] promotional material. Materials may also be distributed to other Program participants, or the public for educational purposes, including but not limited to a Program group photograph of all participants.

Participant Name: _____

Parent or Guardian Name: _____

Signature of Parent/Guardian:_____ **Date:** _____