June, 2015

Dear CyberHigh Camper,

UW-Whitewater’s CyberHigh Camp is just around the corner – July 16th – 17th. A busy and fun two days have been planned, and we are looking forward to meeting you. Following you will find important information about the camp. Please take some time to read it carefully.

Check-in & Check-out

Check-in is scheduled for Thursday, July 16th from 8-8:30 a.m. in Starin Hall on the UW-Whitewater campus. Driving directions and a copy of the UW-Whitewater campus map can also be found at http://www.uww.edu/Campus/. The most convenient parking is in Lot 7.

Check-out will take place from 2:45-3 p.m. on Friday, July 17th in Starin Hall.

*** All remaining fee payments need to be made 10 days prior to camp check-in.

Items to be Completed and Returned at Check-in

Acceptable Use Policy

The safety of your child as well as the other campers is important to us. We are well aware of the concerns that many parents have regarding the use of technology, in particular the Internet. It is our expectation that all campers will use the technology appropriately and for educational purposes. Please read and review the enclosed CyberHigh Acceptable Use Policy with your daughter. A signed copy of this policy must be brought to camp on the first day.

HealthEcamper

Please complete the HealthEcamper online Health Form. This form is required and a link will be emailed to you. Without this form campers will not be allowed to participate in the camp.
Cell Phone Policy

So as not to distract instructors, staff, and other campers, use of cell phones (including texting) during camp is strictly prohibited. If they are not absolutely necessary, we ask that they be left at home. If you need to contact your child during the camp, please call one of the following:

7:00 a.m. – 4:30 p.m. Continuing Education at 262-472-3165 or ITSCM Department at 262-472-1322

4:30 p.m. – 7:00 a.m. Laura Schoenike, Overnight Mentor 920-988-9994

Other Policies/Rules

Please read the enclosed list of CyberHigh policies and rules. These rules will be strictly enforced.

What to Bring

Please review the enclosed list of suggested items to bring to camp. Most of our activities will take place in air-conditioned buildings. Temperatures in these buildings can be cool. You may want to bring a sweatshirt or sweater.

You can also come with ideas! Campers will be working in groups of three to four people to explore technology products/innovation. Time will be provided for groups to brainstorm about technology products/innovations, so it is not essential that you come with ideas. However, it will make the brainstorming and planning much more productive!

We are looking forward to a fun and exciting week. Please remember to complete and return (at check-in) the following the Acceptable Use Policy Form.

If you have any questions, please contact us either via e-mail (techcamps@uww.edu) or via phone (262) 472-1322.

Sincerely

Alana Platt and Sara Deschner

Alana Platt and Sara Deschner
CyberGirlz Camp Committee
2015 CyberHigh Policies & Rules

These rules have been established to make this camp an enjoyable and safe experience for everyone. Any breach of these rules will result in the immediate notification to parents and the student will be dismissed from the camp. Students so dismissed will not receive any refund of camp fees.

1. Smoking, the use of alcohol and other drugs, firearms weapons or fireworks are prohibited. Parents will be notified and violators will be sent home immediately. *There will be no refund of fees for violation of this policy.*

2. All campers are confined to the University campus property; any trips off campus require written permission from the parent and approval of the camp director or head counselor. All campers making off campus trips must be accompanied by a staff member unless written permission from the parent is provided.

3. Any damage to University property by campers will be paid for by the camper or his/her parents.

4. Campers are encouraged to have their own health insurance as limited accident insurance is provided by the University. University insurance coverage is included in your registration and covers you *only while you are on campus and for camp-related accidents.* If you are a commuter, this insurance will *not* cover you while you are traveling to or from camp. Camp insurance does not cover pre-existing injuries.

5. You will be given a meal band that you must bring to every meal. Lost or destroyed bands will be replaced at the dining center at a fee to the camper.

6. Campers are not allowed to enter any residence hall other than the one assigned to their camp. Boys are not allowed to enter girls’ rooms and vice versa. With the exception of check-in and check-out, no visitors are permitted in your room at any time.

7. Campers are responsible for their own money and personal items; *the University and the camp are not responsible for lost items.* **KEEP YOUR DOORS AND LOCKERS LOCKED AT ALL TIMES. DO NOT SHARE YOUR ROOM COMBINATION OR KEYS WITH OTHERS.**

8. There will be no hazing, taunting or teasing of other campers or guests on campus. Violators will be dealt with accordingly.

9. Any camper who is ill or injured should first notify instructors if possible. If not, report to training room inside Williams Center.

11. All campers must be in the residence halls before 11 p.m. when the doors are locked. Lights in your room should be off by 11:15 p.m. sharp. No individuals from other camps or from the community are permitted in the residence hall without permission of the Camp Director.
What to Bring to CyberHigh

☐ Sleeping Bag or Bed Linens
☐ Pillow
☐ Personal Clothing – don’t forget a swimsuit
☐ Towel(s)
☐ Personal Care Items (soap, shampoo, toothbrush, toothpaste, etc.)
☐ Fan (there is no air conditioning in the dorms!)
☐ Alarm Clock
University of Wisconsin – Whitewater CyberHigh Camp Computer Acceptable Use Policy

Please read the following excerpts from the UW-Whitewater Acceptable Use Policy and indicate your agreement to the policy by signing at the end of the document.

Appropriate Use

Listed below are the policies that govern data network access and usage for students, staff and faculty at the University of Wisconsin Whitewater.

1. Authorized users

Authorized users are (1) current faculty, staff, and students of the University; (2) individuals connecting to a public information service supported on the Campus network and (3) others who are specifically authorized to use a particular computing or network resource by the campus unit responsible for the resource.

2. General Guidelines

Those who use the campus network resources are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct.

3. Security

Information security at UW-Whitewater is everyone's responsibility. To maintain security in using the campus network services, it is important to adhere to the following guidelines:

- Protect your login ID and password. Computer accounts, passwords, ids and other types of authorization are assigned to individual users and should not be shared with others.
- Be aware that the person to whom an account is assigned will be held accountable for any activity originating from that account.
- Do not access data or systems for which you have not been given specific authority.
- Take reasonable steps to ensure that your desktop or laptop computer system does not create a security risk when connected to the network, including keeping anti-virus software and operating patches up-to-date.
- Report security violations.

4. Confidentiality

Information stored on computers is considered confidential, whether protected by the computer system or not, unless the owner intentionally makes that information available to other groups or individuals. The University of Wisconsin Whitewater takes the position that computer users desire that the information that they store on central and/or campus shared computing resources remain confidential.
While all efforts will be made to ensure confidentiality, users should be aware that data (including e-mail) might, due to software or hardware failure, become accessible to those who are not explicitly authorized for that access. iCIT personnel may also on occasion have access to such data while performing routine operations or pursuing apparent systems or user problems. No guarantee of complete privacy is made or implied by this policy.

Requests for the disclosure of confidential information will be governed by the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Wisconsin Open Records Statutes (Chapter 19, ss. 19.31 - 19.39, Laws of 1992). All such requests will be honored only when approved by University officials who are the legal custodians of the information requested, or when required by state or federal law, or court order. Users found to be copying, modifying, or otherwise accessing information for which they have not been granted permission may be liable to disciplinary action.

**Unacceptable Use**

Network resources at UW-Whitewater may not be used for unlawful activities, commercial purposes not associated with the University, or uses that violate other University policies or guidelines. The following activities are NOT acceptable use of the campus network resources:

- Damaging or performing unauthorized removal of networking equipment, software or data
- Tampering with network hardware, wiring, or software
- Disrupting or interfering with the normal operation of network communications, generating excessive network activity or performing unauthorized monitoring of network traffic
- Willfully introducing computer viruses or other disruptive programs into the university network, which are intended to damage or create excessive load on network resources
- Intentionally violating or attempting to bypass network security strategies
- Using unauthorized accounts, passwords, IP addresses or other network access information
- Accessing or modifying any software, files, data or other university information for which an individual has not been given authorization
- Using network resources to harass or intimidate others
- Using network resources to impersonate others or to forge another's identity
- Interfering with the computing activities of others.
- Setting up network services or equipment without knowledge or involvement of iCIT.
- Violating state, federal or copyright laws
- Using network resources for commercial activity or financial gain which does not conform to UW-W rules and regulations.

I have read the above policy and agree to abide by the terms listed.

___________________________________  ______________
Student       Date

___________________________________  ______________
Parent/Guardian     Date