Welcome to the Duquesne University Cyber Ethics Conference!

On Monday, October 1st, 2012, in conjunction with Freshman Orientation week, Duquesne University will be hosting a Cyber Ethics conference and panel discussion with Keynote speaker, Lawrence Lessig, Harvard Law Professor and Author. Over 1,500 freshmen, distinguished panel members, faculty and guests will be in attendance for this event to explore the many nuances of Cyber Ethics. Funding for this program is being sponsored by Duquesne University President Charles J. Dougherty, Ph.D. and Dr. Olga M. Welch, Dean of the School of Education. The Chair of our panel discussion is Dr. Darren Mariano, Adjunct Professor of Cyber Ethics at Duquesne University.

As a requisite for introduction into collegiate life, all incoming freshmen are required to attend each session of the conference. In appreciation of your attendance at these breakout sessions, a scavenger hunt will be conducted with clues across the campus. Top prizes include iPhone 5s, iPad 3s, Galaxy Tablets and Droid Smart Phones.

Benefits of Digital Literacy: Cyber Ethics, Network Safety and Security

The goal of this conference is to serve as a point of enlightenment for our students, faculty, and support personnel to share educational schemas, current research and expertise in cyber ethics and its implications for the members of our academic community.

Description

The broad range of topics to be presented includes cyber ethics, Internet safety, identity theft, cyber-bullying, the University’s code of conduct and policy regarding Academic Integrity. These topics include recent research and legislative actions designed to promote the responsible use of online technology and multimedia in a safe and conscientious manner.
Conference Highlights

Knowing Your Network

- Privacy
- Online Personas

Cyber Safety

- Cyber-Bullying
- Cyber-Stalking

Living Up to the Code

- Code of Conduct/Academic Integrity (Plagiarism & Intellectual Property)
- Web Etiquette
- Network Safety

Keynote Address

Getting to Know the Community: Panel Discussion

Closing Remarks
Duquesne University Cyber Ethics Conference Agenda
October 1, 2012

Registration, Material Collection, & Continental Breakfast

8:00-8:30a | Location: Options Cafe (5th floor of Duquesne Union)
Students can fill out nametags for the day and collect a folder, which contains the days itinerary, handouts and breakout group assignment. A continental breakfast of donuts, muffins, juice and coffee will be provided for students to enjoy while they mingle with other attendees.

SESSION 1

Knowing Your Network

8:30-10:15a | Location: Duquesne Union Ballroom
This introductory session is designed to be interactive with our student participants. This session will be led by an expert member of the Cyber Security Team. There is a growing concern regarding privacy issues on the Internet. In this primary session, the topic of Knowing Your Network will provide the necessary guidelines to securing personal information in a cyber-society. This session will also include the impact and associated risks regarding the creation of social identities known as online personas. A goal of this session is to provide a foundational understanding of these issues to prepare students for the remainder of the day's breakout sessions.

Break 10:15-10:30a
Use this time to make your way to your breakout session location. This information can be found in your conference folder.

SESSION 2

Cyber-Bullying and Cyber Stalking

10:30-12:00p | Location: Various locations for breakout groups
The topic of Cyber Safety will be covered in small group breakout sessions that will be held at various locations throughout campus. Each session will consist of approximately 25 students and
will be led by an upper-class student helper, such as a resident assistant, who has been specially trained for this event.

Group leaders will focus on each student’s individual role and responsibilities in practicing and promoting ethical behavior in cyber-space. Specific behaviors and strategies will be identified so that students will be able to take away from this session appropriate actions which can be implemented and applied to their daily lives.

Activities during this session are designed to present the topic of cyber-bullying and cyber-stalking on a level that connects with today’s college students and will include small group discussion and interaction with the aid of mobile devices and social media.

**Lunch Break**
12:00-1:00p | Various locations for breakout groups (catered by Food Services)

**SESSION 3**

**Living Up to the Code**
1:00-2:45p | Location: Duquesne Union Ballroom

Living Up to the Code will be a comprehensive look at how our actions on the Internet effect the way we are perceived by our peers, instructors and future employers. This session will cover Duquesne University's Code of Conduct policy, including discussions on Academic Integrity, Plagiarism, and Intellectual Property. Lastly, learning how to navigate a network of users safely can be tricky; this topic will outline how one can protect their identity and personal information while on the Internet.

Topics covered as followed:
- Code of Conduct/Academic Integrity (Plagiarism and Intellectual Property)
- Web Etiquette
- Network Safety

**Break 2:45-3:00p**
SESSION 4

Keynote Speaker: Lawrence Lessig, Harvard Law Professor and Author

3:00-3:30p | Location: Duquesne Union Ballroom

Lawrence Lessig in one of the nation's leading authorities on legal issues with technology and cyberspace. He is the Director of the Edmond J. Safra Foundation Center for Ethics at Harvard University, and a Professor of Law at Harvard Law School. He is the author of five books on law and technology; including most recently, *Remix* (2008) and *Code V2* (2007).

This presentation will focus on the *Remix Culture* and the legalities behind creating and sharing through the Internet.

SESSION 5

“Getting to Know the Community”

3:30-4:30p | Location: Duquesne Union Ballroom

The panel brings together professionals from the Duquesne University community to discuss the major issues surrounding cyber ethics on Duquesne University and what individuals can do to keep themselves safe and better prepared. Panelists will be representatives from a variety of offices and departments on campus, and will inform students on the services their office offers in relation to the topics discussed. The panelists will provide students with tips on how to deal with some of these issues and invite participation from the audience during a question and answer session at the end of the presentation.

Participants

- Chair: Dr. Darren G. Mariano, Adjunct Professor in Cyber Ethics
- Susan Monahan, Director of Student Conduct
- Tom Hart, Director of Public Safety
- John Ziegler, Executive Director of Computing & Technical Services (CTS)
- Dr. Ian C. Edwards, Director of the Counseling Center
- Sharon Oelschlager, Director of Residence Life

SESSION 6

Closing Remarks

Dr. Darren G. Mariano will provide closing remarks and highlights from the sessions regarding learner achievement and post-assessment validation of the conference’s effectiveness.
Organizer Plan - How the Sessions will be conducted

Pre-Conference Agenda

Student Helper Orientation
10:00am - 12:00pm, day before the Cyber Ethics Conference presentation
Location: Conference room, Power Center

Student helpers will be guided through an orientation session detailing their role and duties during the Freshman Cyber Ethics Orientation Program. Topics covered will include:

- Overview of topics that the student helpers will be responsible for covering during the "Cyber Safety" breakout session.
- Strategies for facilitating group discussion.
- Goals for what should be accomplished during the "Cyber Safety" breakout session.

At the conclusion of this orientation session, a lunch of free pizza will be provided for all student helpers.

Conference Agenda

SESSION 1
Knowing Your Network
Session Format: Interactive Presentation (PowerPoint & Audience Participation)

*Privacy*: At no other time in our global history has the collection and dissemination of personal information been so readily available. Technology has made it possible to exchange personal information in unprecedented ways to dubious purveyors of such knowledge. There is an increased potential to breach the right to privacy of individuals and groups regardless of location. Securing your personal information is paramount in a cyber-society. Precautions should be taken to ensure the accuracy of the data with an ability to review stored information and correct inaccuracies. Respect for confidentiality is an ethical concern. A dilemma arises when confidential content is disclosed without the knowledge or consent of the owner. The provisions of the Fourth Amendment include freedom from intrusion, control of information (personal) and freedom from surveillance. Private information includes any information by which a living individual can be identified. This information also pertains to photos. Participants will be shown the *Ethics of Internet Privacy*
http://www.youtube.com/watch?v=tD4_gJwfCMM&feature=related
**Online Personas:** In cyber terms, a persona is a social identity which individuals create to interact in cyber communities when engaging in social media activities. This alter ego can be quite persuasive. Trouble ensues when the alter ego becomes the dominant part of a person’s personality or when potential employers see this other side of an individual perceived in a less than positive light. Further issues can arise in chat rooms where a person's physical characteristics can be misrepresented leading to inaccurate perceptions regarding the communicator's age, gender, beliefs etc. which can result in a victimization scenario ensuing.

**SESSION 2**

**Cyber-Bullying and Cyber Stalking**

*Session Format: Breakout Groups*

**Some characteristics of cyber-crime techniques are listed below:**

- Physical location is no longer a requirement for a crime to be committed. The perpetrator and his victim can be across the street, in the next county, across interstate lines or in another country halfway around the globe.
- Technology enables crimes without borders.
- Multiple victims can be attacked automatically at an accelerated rate.
- Anonymity is significantly increased in a cyber-crime.

The targets and types of crimes in the physical world do not differ much from those in the cyber world: burglary, theft, deception, extortion, fraud, and identity theft and child exploitation are still evident in cyberspace. What changes are the techniques, the choice of weapon, the augmented opportunities, and the exponential increase in victims, the degree of traceability of cyber fingerprints and the location of the perpetrator compared to the location of the victim. The Internet provides criminals with the means to target their victims remotely. Unlike crimes in the physical world where the encounters are often face-to-face and experienced on a very personal level, cyber criminals prefer a more stealthy approach. Under the radar, they can perpetrate their crimes without leaving the typical clues behind such as finger prints or other physical evidence for law enforcement to recreate the crime scene. By using multiple networks and interrelated computers, the reverse trail is often very difficult to recreate and trace. Exploitation vs. disruption has become the pattern for the dark side of the Internet. An overlap exists between organized crime and individuals who use botnets and zombies to execute their cyber crime activities. The correlation exists between the early days of the brick-and-mortar companies moving to the Internet in search of profits and growth of their customer base and those of criminal ventures intent on a similar purpose of illegal enterprises and activities.

**Cyber-Bullying:** In this session, we will address the 3C's of Inappropriate Contact, Content, and Conduct as defined in the most recent addition to the OnGuardOnline.gov campaign.  

A cyber-bully is one who intentionally uses internet technology or cellular services to send inflammatory, threatening or harassing text messages, emails or inappropriate images to their targeted victim. The content of the emails can include false statements, rumors, or hate messages against a person's religion, physical appearance or features, sexual orientation, ethnicity or race.
These text messages, emails, photos and other inflammatory and derogatory materials may also be posted on social networking sites, or as videos.

Students will be shown the Cyber-Bullying "Cliques and Click" video. 
http://www.youtube.com/watch?v=xY6MoiDRwqU&feature=related

**Cyber-Stalking:** Cyber-stalking is an extension of cyber-bullying. A cyber-stalker is considered a "creep" who intimates his or her victims through their presence on the web and often operates in the shadows of cyber-space. The profile of a cyber-stalker is very similar to an off-line stalker. Their goals of power and control, intimidation and the intent to cause fear and uncertainty in their victims do not change. Cyber-stalking is considered to be an adult action where cyber-bullying is more related to negative adolescent behavior.

**Anti-Stalking Tips provide by the Norton Security Center**
http://us.norton.com/cyberstalking/article

Here are a few important pointers to help you thwart cyber-stalking, whether it's directed at you, your PC, or your family:

- Maintain vigilance over physical access to your computer and other Web-enabled devices like cell phones. Cyber-stalkers use software and hardware devices (sometimes attached to the back of your PC without you even knowing) to monitor their victims.
- Be sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password. The same goes for passwords on cell phones. Your kids and your spouse should develop the same good habits.
- Make sure to practice good password management and security. Never share your passwords with others. And be sure to change your passwords frequently! This is very important.
- Do an online search for your name or your family members' now and then to see what's available about you and your kids online. Don't be shy about searching social networks (including your friends' and colleagues'), and be sure to remove anything private or inappropriate.
- Delete or make private any online calendars or itineraries--even on your social network--where you list events you plan to attend. They could let a stalker know where you're planning to be and when.
- Use the privacy settings in all your online accounts to limit your online sharing with those outside your trusted circle. You can use these settings to opt out of having your profile appear when someone searches for your name. You can block people from seeing your posts and photos, too.
- If you suspect that someone is using spyware software to track your everyday activities, and you feel as if you're in danger, only use public computers or telephones to seek help. Otherwise, your efforts to get help will be known to your cyber-stalker and this may leave you in even greater danger.
- As always, use good, updated [[/products|security software]] to prevent someone from getting spyware onto your computer via a [[/security response/phishing.jsp|phishing]] attack or an infected Web page. Check the app store for your mobile devices to see what security software is available. Or visit the Norton Mobile page to see what programs are
available for your device's platform. Security software could allow you to detect spyware on your device and decrease your chances of being stalked.

As an introduction to these next topical areas, participants will view the *Cybercrime and Cyber Ethics* video. [http://www.youtube.com/watch?v=BKR9uP0-W_8](http://www.youtube.com/watch?v=BKR9uP0-W_8)

**SESSION 3**  
**Living up to the Code**  
*Session Format: Interactive Presentation (PowerPoint & Audience Participation)*

**Code of conduct/Academic Integrity (Plagiarism & Intellectual property):** This is a topic that is outlined in every class on every syllabus. The speaker will review the code of conduct and talk about the ins and outs of plagiarism.

**Web etiquette:** Knowing how to play nice in the online sandbox is a crucial part of the business (and social) world. Netiquette is a blend of the words network and etiquette. It is the culture of how people communicate and interact through online networks. Topics will include avoiding offensive language or behavior, using proper grammar and editing techniques, considering and respecting the privacy of others, avoiding “Leet speak,” and not getting involved in flame wars.

**How to Follow Proper Netiquette Rules** [http://www.youtube.com/watch?v=6dRoclqDJh0](http://www.youtube.com/watch?v=6dRoclqDJh0)

**Network Safety:** Network Safety is all about being educated about the multiple dangers the online world presents. There are many free online brochures at the Microsoft Security website. ([http://www.microsoft.com/security/online-privacy/social-networking.aspx](http://www.microsoft.com/security/online-privacy/social-networking.aspx)) They outline the eleven steps for social networking safety:

1. Use caution when you click on links that you receive in messages from your friends on your social website.
2. Know what you've posted about yourself.
3. Don't trust that a message is really from who it says it's from.
4. To avoid giving away email addresses of your friends, do not allow social networking services to scan your email address book.
5. Type the address of your social networking site directly into your browser or use your personal bookmarks.
6. Be selective about who you accept as a friend on a social network.
7. Choose your social network carefully
8. Assume that everything you put on a social networking site is permanent.
9. Be careful about installing extras on your site.
10. Think twice before you use social networking sites at work.
11. Talk to your kids about social networking.

**Identity Theft:** This type of theft is the wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.
**Phishing Scams:** A phishing scam is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information. As complex technology has evolved, it has become much simpler for cyber criminals to perpetrate their crimes. Rather than serving as a deterrent to criminals by requiring a higher level of knowledge, enhancements in technology have actually made it easier for cyber-attacks to occur. Less knowledge is now required by the perpetrators because intrusion tools have become more sophisticated. For example, the types of crimes also evolved from simple password guessing to distributed attack tools: correspondingly, sweepers, sniffers, and network diagnostic capabilities enhanced their attack strategies.

Cyber-crime continues to evolve into the exploitation of software vulnerabilities, distribution of multiple viruses and worms, and continued multi-pronged attacks from numerous rogue servers. Looking towards the future, a projected trend for the next decade would be the continued evolution of botnets which coordinate attacks on behalf of more sophisticated cyber criminals. Less sophisticated hackers will continue to use the tools which are widely available and distributed over the Internet. These hackers will be exposed using commercial grade software such as COTs (Commercial off-the-shelf) whereas the more sophisticated cyber criminals may be detected by using theoretical methods still in development at the institutional and government levels.

**Computer Viruses, Worms and Trojan Horses:**

Self-replicating programs (Slammer, Melissa, ILOVEYOU, Bugbear, Code Red, SirCam, Nimda, Morris etc.) are code fragments that attach themselves to other programs (viruses) or machines (worms). Viruses and worms attempt to shut down networks by flooding them with massive amounts of spurious traffic, usually through email. Enhanced protection systems such as McAfee and Symantec have provided a better defense against these types of attacks. Microsoft has also been held more accountable to provide better security updates for their software in parallel with other antivirus companies competing for market share. When the unsuspecting user downloads the Trojan horse, it launches a virus, password gobbler, or remote control software (the hacked software) that enables the hacker to gain control of the PC. They are the leading cause of all break-ins and are attached to other programs. A correlation exists between the types of cyber-crimes committed and the increased use of e-commerce. The frequency of some cyber-crimes are being contained by more effective Intrusion Detection Systems (IDS), regulatory compliance, corporate governance and risk auditing procedures. In the private sector, security and information assurances remain fundamental challenges.

**SESSION 4**

**Keynote Speaker**

Session Format: Interactive Presentation (PowerPoint & Audience Participation)

Lawrence Lessig is one of the nation's leading authorities on legal issues with technology and cyberspace. He is the Director of the Edmond J. Safra Foundation Center for Ethics at Harvard University; and, a Professor of Law at Harvard Law School. He is the author of five books on law and technology; including most recently, *Remix* (2008) and *Code V2* (2007). This
presentation will focus on the *Remix Culture* and the legalities behind creating and sharing through the Internet.

In Lessig's 2008 book, *Remix*, he explains that our culture has moved from a "read only" culture to a "read/write" culture. In a Read Only culture, professionals and experts in a field create content that is accessible to the masses in a read only form meaning they have no way of interacting with the information. They can simply take the information in as is. In a read/write culture, the consumer has the ability to *remix* the content created by the original author. They can add to it, take away from it, merge it with content from another source, etc. Lessig argues that this type of culture, which allows for all consumers to be producers as well, is essential in advancement. Copyright issues arise when dealing with a read/write culture. In this presentation, Lessig will discuss current copyright laws, the future of copyright laws, and how students can work within the current laws.

**SESSION 5**  
**Getting to Know the Community: Panel Discussion**  
*Session Format: Panel Presentation (Panel/Q&A)*

Dr. Darren G. Mariano will open the session with an introduction about the goals of the panel and allow the panelist to briefly introduce themselves. After the completion of the introductions, each panelist will be given 5 minutes to discuss the role of their office in regards to issues related to cyberspace. At the completion of the mini presentations, students will be allowed to ask questions to the panelists. If there are no immediate questions, Dr. Mariano will have a few ethical situations (related to realistic events that could happen to a university student) and allow the respective panelist to speak on behalf of their department on how students could best handle that situation. There will be a projector screen, which will display the hashtag #DUethics in TweetChat (a live feed of a specific Twitter hashtag). Students will be allowed to tweet in questions to the panelists, respond to questions asked by the panelists and provide a back channel for archiving purposes.

*Susan Monahan, Director of Student Conduct*

- Understanding your own moral, ethical and spiritual values and principles
- Rights as members of the academic community, protection from unfair disciplinary action
- **Student Code of Conduct:** Lying, Stealing, and Identification Misuse, Harassment or discrimination, computer Misuse, attempted or actual theft or other abuse of computer time, or computing facilities access.

*Tom Hart, Director of Public Safety*

- Failure to report illegal activity and/or violation of the Code of Student Rights, Responsibilities and Conduct.
- Irresponsible social conduct that does not reflect the Mission and Expectations of the University whether on or off campus.
John Ziegler, Executive Director of Computing & Technical Services (CTS)

- Unauthorized entry, transfer, or altering files.
- Unauthorized use of another individual’s identification and/or password.
- Use of computing technology to interfere with work of another student, faculty, or University official as well as the normal operation of the University infrastructure in accordance with the

Mission of the University:

- Use of computing resources and facilities to send obscene, harassing, or abusive messages.
- Use of computing resources and facilities for fraudulent acquisition of goods or services, conducting activity for private profit or in violation of any published University regulations.
- Use of computing facilities and resources in violation of copyright law.

Dr. Ian C. Edwards, Director of the Counseling Center

- Will cover what to do if you are the victim of the aforementioned abuse, or misuse, and will cover the types of services offered: personal counseling, group counseling, consultation, and workshops.

Sharon Oelschlager, Director of Residence Life

- Address the role of victim or perpetrator of any of the previously mentioned acts with specific intent to Residence Life Policy.
- Residence Life’s role as a monitor of web content contents with students’ report of online violations to the Office of Residence life; addresses the process for handling various issues in the residence halls; and, judicial action in the resident director hearings.

SESSION 6
Closing Remarks
Dr. Darren G. Mariano will close the conference with a summation of the essence of learner achievement for each section as a post-assessment for validation of the conference. Students will be advised of an online evaluative assessment tool they are to complete as a final step in their orientation to Duquesne University. The subsequent results analysis will identify the impact on learners and the impact on the University to sponsor similar conferences in the future.