CYBERSECURITY

privacy, ethical implications

1. DURING ON-LINE ACTIVITIES NOBODY IS UNKNOWN. THERES ALWAYS A CHANCE THAT ONLINE ACTIVITIES CAN BECOME PUBLIC.

2. ORGANIZE ON-LINE ACTIVITIES IN SUCH WAY THAT ACCESS IS LIMITED ONLY TO VERIFIED USERS.

3. USE ONLY APPS AND PLATFORM IN THE CLASSROOM OR ON-LINE THAT WERE APPROVED BY YOUR INSTITUTION.

4. ALWAYS USE STRONG PASSWORDS FOR EDUCATIONAL APPS AND PLATFORMS.

5. DONT USE PERSONAL EMAIL TO TRANSFER STUDENT DATA. WHEN ADDING STUDENTS TO A VIRTUAL CLASSROOM, ALWAYS CONFIRM IDENTITIES.

6. ENSURE A CYBER-SAFE CLASSROOM AND PROTECT STUDENTS' PRIVATE DATA. IF ANY THIRD-PARTY IS INCLUDED IN SHARING DATA, MAKE SURE THAT EVERYBODY ARE AWARE.

7. IF CLASSES ARE RECORDED MAKE SURE THAT EVERYBODY AGREE TO THAT BEFORE DOING SO.

8. IF YOU SHARE YOUR VIDEO AND VOICE KEEP IN MIND THAT BACKGROUND IS ALSO SHARED.

9. THERE IS ALWAYS A POSSIBILITY THAT SOMEBODY IS RECORDING.

10. TEACH STUDENTS THE BASICS OF ONLINE PRIVACY AND SECURITY.

11. ENSURE TECHNOLOGY IN CLASS IS A BENEFIT, NOT A DISTRACTION.

12. CUT DOWN ON MULTITASKING. FOR EXAMPLE, AVOID FORCING STUDENTS TO FOCUS ON LISTENING AND WRITING, OR SOLVING TASK SIMULTANEOUSLY.

13. DIGITAL CONTENT: USE SHORT PARAGRAPHS, SCANNABLE TEXT, BULLETS, IMAGES AND VIDEOS TO HELP VISUALIZE.

14. HAVING DETAILED LECTURE NOTES REMOVES THE INCENTIVE TO PAY ATTENTION IN CLASS.

15.NOTHING IS FOR FREE. IF YOU USE FREE SOFTWARE OR APP, CONSIDER THAT YOU MIGHT BE A PRODUCT.

16.ASK AND LISTEN STUDENTS CONCERNS.