

Basic *Children's Internet Protection Act* (CIPA)

— R E Q U I R E M E N T S —



PARTICIPANT'S GUIDE

Grade 6



Stage 1

ONLINE SAFETY REQUIREMENTS

BAKERSFIELD CITY SCHOOL DISTRICT
1300 Baker Street
Bakersfield, CA 93305

ACCEPTABLE USE AGREEMENT (AUA):
DISTRICT TECHNOLOGICAL RESOURCES

Background Information, Commitments, and General Requirements

The Governing Board of the Bakersfield City School District's ("District") has adopted a policy (Student Use of Technology, BP 400.43) describing rules and procedures to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of, or access to, sensitive information, and to comply with the: (1) Children's Online Privacy Protection Act (15 USC 6501-6506 & 47 CFR 312.1-312.12); (2) Broadband Data Improvement Act. (Pub.L. 110-385.); (3) Protecting Children in the 21st Century Act (15 USC 6551); (4) Children's Internet Protection Act (20 USC 6301 et seq); (5) Enhancing Education Through Technology Act of 2001 (20 USC 6751 et seq.); and (6) the internet safety provisions of the No Child Left Behind Act (20 USC 6777). This *Acceptable Use Agreement (AUA)* brings together information from several District policies describing user obligations and responsibilities. The term "user" means anyone using District technological resources (e.g., computers, Internet, email, other forms of direct electronic communications, and equipment provided by the District regardless of the physical location of the user).

The District will use technology protection measures to block or filter, to the extent possible, access of visual depictions that are *obscene, pornographic, and harmful to minors* over the network. The District reserves the right to monitor use of the District's technology resources for improper use without advance notice or consent and to take immediate corrective action regarding any improper activities. As the District deems necessary, authorized employees will: (1) monitor users' online activities; (2) access, review, and copy; (3) store or delete any electronic communication or files; and (4) disclose files and documents to others. Users have no expectation of privacy regarding their use of District technological resources.

Users shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on race or ethnicity, ethnic group identification, physical or mental disability, medical condition, marital or parental status, sex or gender, gender identity, gender expression, genetic information, age, color, ancestry, national origin or nationality, religion, limited proficiency in English, or sexual orientation.

District staff will provide age-appropriate instruction to students about the safe, proper, and appropriate behavior while using technological resources. Although student use of District technological resources to access public social networking sites is prohibited, such instruction shall include, but not be limited to: the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, interacting with other individuals on social networking web sites and in chat rooms, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Use of District Technological Resources

Before a student is authorized to use the District's technological resources, the student and his/her parent/guardian shall sign and return this *AUA* to acknowledge and agree to all the conditions specified here. Each District school will keep a copy of the *AUA* signature page on file. Annually and before each student uses District technology, the principal/designee will verify the presence of a fully executed *AUA*. Once signed, the *AUA* acknowledgement/permission page remains in effect until: (1) revoked by the parent; (2) the student has a cancellation of user privileges; or (3) the student is no longer enrolled. Even without a signature on the *AUA*, employees, students, and all other users are required to follow applicable laws, policies, procedures, including

the requirements described within this *AUA*. By using the District resources, each user agrees to comply with all rules. Each user is required to report any misuse of the District's technological resources to the appropriate employee (e.g., teacher, supervisor, or other District personnel). If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor, or other appropriate District personnel.

Students are authorized to use District technological resources or equipment to access the Internet or other online services in accordance with Board policy, the user obligations, and responsibilities specified in the District's *Acceptable Use Agreement*.

Accessing Technological Resources Outside of School Setting. Students will access the District technological resources outside of school only if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use outside of school.

Penalties for Improper Use

Students who violate District or school rules and regulations, to include the unacceptable uses of the District's technological resources may be subject to consequences including, but not limited to: (1) legal action; (2) suspension; (3) expulsion; (3) transfer to alternative programs; (4) cancelling or limiting student user privileges; (5) denial of participation in extracurricular or cocurricular activities; (6) or other privileges. When a crime may have been committed, the Superintendent or designee shall notify local law enforcement. In accordance with law and policy, students also may be subject to a District or school consequence(s), for any off-campus conduct during non-school hours that poses a threat or danger to the safety of students, staff, or District property, or substantially disrupts school activities.

Disclaimer

The District makes no guarantees and denies any responsibility for the accuracy or quality of the information obtained by using District technological resources. Any statement accessible through the District's resources is understood to be the author's individual point of view and not that of the District, its affiliates, or employees. The student and parent/guardian, as a condition of the student's use of District technological resources, agree to indemnify and hold harmless the District or any District employee and waive all claims or suits for damages, costs, or injury arising from the failure of any technology protection measures, violations of copyright restrictions, user mistakes or negligence, or other obligations arising from use of District technological resources. Any charges a user accrues due to the inappropriate and unauthorized use of the District's resources are to be borne by the user.

**BAKERSFIELD CITY SCHOOL DISTRICT:
ACCEPTABLE USE AGREEMENT
ADDITIONAL STUDENT AGREEMENTS**

Personal Responsibility and Safety

1. I will use the school computers safely, responsibly, and for educational purposes.
2. I will take care of the computer and all technology equipment as if it belonged to me.
3. I will keep my passwords private and not share them with my friends.
4. I will only use school computers for classroom work assigned by the teacher.
5. I will report any misuse of the computer or the network to a teacher or the principal.
6. I will immediately stop and tell the teacher or person in charge if anything happens on the computer or on the Internet that is wrong or makes me feel uncomfortable.

Inappropriate Uses

7. I will not use someone else's username and password to log into the computer or network.
8. I will not read, delete, copy, or modify email or use another person's identity.
9. I will not attempt to bypass security measures on the District network.
10. I will not download any software from the Internet unless specifically directed to as part of a lesson.
11. I will not buy, sell, or advertise anything using the school computer and/or network.
12. I will not use technology equipment to encourage the use of drugs, alcohol, and tobacco or take any action that is unethical or prohibited by law or District policy.

Digital Citizenship

13. I will not threaten, harass, insult, ridicule, gossip, or tease others while I am online or using a computer. I understand these behaviors may result in punishment to include loss of privileges.
14. I will not copy information and use it as if it were my own ideas without giving credit to the information's author and source. I know that failure to properly cite my sources of information is called plagiarism and is a form of cheating.

Online Behavior

15. I understand that computer files and electronic communications are not private and may be accessed by the District to ensure proper use.
16. I will not share personal information (either my own nor another student's) including: references to where I live, details about family or friends (including names), my age, birthday, home address, or telephone number on the Internet.
17. I will use respectful and appropriate language without swearing, name calling, or causing others to feel uncomfortable due to their gender, race, appearance, behavior, or beliefs. (These are actions that could be considered harassment or bullying).
18. I will not post copyrighted material online.

Required Signatures: BCSD Acceptable Use Agreement

STUDENT

By signing below, I am showing I understand and agree to follow all rules listed in this four-page *Acceptable Use Agreement*. I understand that any rules I do not follow may result in disciplinary action, losing my user account, and legal action. I further understand I may be held responsible for using technological resources outside of school if my conduct violates District rules. I agree to report any misuse of the District electronic system to a teacher, principal, or other District employee.

Student Name (please print): _____

Student Signature _____ Date _____

PARENT OR GUARDIAN

As the parent/guardian of this student, I have read and understand this *Acceptable Use Agreement (AUA)* consisting of four pages. I understand this *AUA* has been designed to help ensure safe, proper, and appropriate conduct while staff and students use technological resources. By signing below, I am consenting to my student using District technological resources consistent with all the provisions of this *AUA*. I further understand I may revoke this consent in writing, but this revocation will not affect any action taken in reliance on my consent before the District receives my written notice of revocation.

Parent or Guardian Name (please print): _____

Signature _____ Date _____

SPONSORING TEACHER

I have received and read Board Policy 400.43 entitled Student Use of Technology, the accompanying administrative regulation, and this *Acceptable Use Agreement (AUA)* describing expectations for the appropriate use of the District’s technological resources. I have been provided with information about the role of staff to supervise student use of technological resources. As the sponsoring teacher, I agree to instruct the student to fulfill the requirements of the policy and *AUA*. This commitment includes agreeing to report any prohibited use or misuse of the District’s technological resources to the appropriate Bakersfield City School District administrator and to comply with all applicable law, policy, and procedure.

Teacher’s Name (please print): _____

Signature _____ Date _____

BAKERSFIELD CITY SCHOOL DISTRICT
1300 Baker Street
Bakersfield, CA 93305

ACUERDO DEL USO ACEPTABLE (AUA):
RECURSOS TECNOLÓGICOS DEL DISTRITO

Información de los antecedentes, compromisos, y requisitos generales

La mesa directiva gobernante del Distrito Escolar de la Ciudad de Bakersfield (“Distrito”) ha adoptado una norma (Uso de tecnología del estudiante, BP 400.43) describiendo las reglas y procedimientos para prevenir el acceso no autorizado y otras actividades ilícitas por usuarios en línea, prevenir la divulgación no autorizada, acceso, información sensitiva, y para cumplir con: (1) Decreto de Protección de la Privacidad En Línea de los Niños (15 USC 6501-6506 & 47 CFR 312.1-312.12); (2) Decreto del Mejoramiento de Datos de Banda Ancha. (Pub.L. 110-385.); (3) Decreto Protegiendo a los Niños en el Siglo XXI (15 USC 6551); (4) Decreto de Protección de Internet de los Niños (20 USC 6301 et seq); (5) Decreto de Mejoramiento de la Educación Por Medio de la Tecnología del 2001 (20 USC 6751 et seq.); y (6) y las provisiones de seguridad del Internet del Decreto Ningún Niño se Quedará Atrás (20 USC 6777). Este *acuerdo del uso Aceptable (AUA)* une la información de varias normas del distrito describiendo las obligaciones y responsabilidades del usuario. El término "usuario" significa cualquier persona usando los recursos tecnológicos del distrito (ej., computadoras, Internet, correo electrónico, otras formas de comunicaciones electrónicas directas, y equipo proveído por el distrito a pesar de la ubicación física del usuario).

El distrito usará medidas de protección de tecnología para bloquear o filtrar, hasta el punto posible, acceso de descripciones visuales que son *obscenas, pornográficas, y dañinas para los menores* en la red informática. El distrito reserva el derecho de monitorear el uso de los recursos de tecnología del distrito por uso impropio sin aviso de anticipo o consentimiento y tomar una acción correctiva inmediata respecto a cualquier actividad impropia. Como el distrito considere necesario, los empleados autorizados: (1) monitorearán las actividades en línea de los usuarios; (2) conseguirán acceso, revisarán, y copiarán; (3) almacenarán o borrarán cualquier comunicación electrónica o archivos; y (4) divulgarán archivos y documentos a otros. Los usuarios no tienen expectativa de privacidad respecto a su uso de recursos tecnológicos del distrito.

Los usuarios no deberán conseguir acceso, anunciar, someter, publicar, o mostrar cuestiones dañinas o inapropiadas que sean amenazadoras, obscenas, perturbadoras, o sexualmente explícitas, o que podrían ser interpretadas como acoso o menosprecio de los demás basado en la raza o etnicidad, identificación de grupo étnico, discapacidad mental o física, condición médica, estado civil o paternal, sexo o género, identidad de género, expresión de género, información genética, edad, color, ascendencia, origen nacional o nacionalidad, religión, aptitud limitada en inglés, u orientación sexual.

El personal del distrito proveerá instrucción de edad apropiada a los estudiantes acerca del comportamiento seguro, propio y apropiado mientras usan los recursos tecnológicos. Aunque el uso de los recursos tecnológicos del distrito del estudiante para conseguir acceso a sitios de redes sociales públicos es prohibido, tal instrucción deberá incluir, pero no estará limitada a: los peligros de anunciar información personal en línea, mala representación por depredadores en línea, cómo reportar amenazas o contenido inapropiado u ofensivo, interactuar con otros individuos en sitios de redes sociales y salas de charlas, comportamientos que constituyen acoso cibernético, y cómo responder cuando se es sujeto al acoso cibernético.

Uso de los recursos tecnológicos del distrito

Antes de que un estudiante sea autorizado para usar los recursos tecnológicos del distrito, el estudiante y su padre/madre/tutor deberá firmar y regresar este Acuerdo del uso aceptable (*AUA*) para reconocer y estar de acuerdo a todas las condiciones especificadas aquí. Cada escuela del distrito mantendrá una copia de la página

de la firma del *AUA* archivada. Anualmente y antes de que un estudiante use la tecnología del distrito, el director/designado verificará la presencia de un *AUA* totalmente ejecutado. Una vez firmada, la página de reconocimiento/permiso del *AUA* permanecerá en efecto hasta que: (1) sea revocada por el padre/madre; (2) el estudiante tenga una cancelación de privilegios de usuario; o (3) el estudiante ya no esté inscrito. Aún sin una firma en el *AUA*, a los empleados, estudiantes, y todos los demás usuarios se les requiere seguir las leyes aplicables, normas, procedimientos, incluyendo los requisitos descritos dentro de este *AUA*. Usando los recursos del distrito, cada usuario está de acuerdo con cumplir con todas las reglas. A cada usuario se le requiere reportar cualquier uso incorrecto de los recursos tecnológicos del distrito al empleado apropiado (ej., maestro, supervisor, u otro personal del distrito). Si el usuario no está seguro acerca de si un uso particular es aceptable o apropiado, él o ella deberán consultar a un maestro, supervisor, u otro personal apropiado del distrito.

Los estudiantes están autorizados para usar los recursos tecnológicos del distrito o equipo para conseguir acceso al Internet u otros servicios en línea en conformidad con la norma de la mesa directiva, las obligaciones del usuario, y responsabilidades especificadas en el *Acuerdo del uso aceptable* del distrito.

Conseguir acceso de recursos tecnológicos fuera de la ubicación de la escuela. Los estudiantes conseguirán acceso a los recursos tecnológicos del distrito fuera de la escuela sólo si un padre/madre o tutor legal supervisa su uso en todo momento. El padre/madre o tutor del estudiante es responsable por monitorear el uso del menor fuera de la escuela.

Consecuencias por el uso impropio

Los estudiantes quienes violen las reglas y el reglamento del distrito o escuela, que incluye los usos inaceptables de los recursos tecnológicos del distrito pueden estar sujetos a consecuencias incluyendo, pero no limitadas a: (1) acción legal; (2) suspensión; (3) expulsión; (3) transferencia a programas alternativos; (4) cancelar o limitar los privilegios de usuario del estudiante; (5) denegación de la participación en las actividades extracurriculares o co-curriculares; (6) u otros privilegios. Cuando un crimen pudo haber sido hecho, el superintendente o designado deberá notificar a las autoridades policíacas locales. De acuerdo con la ley y norma, los estudiantes también pueden estar sujetos a las consecuencias del distrito o escuela, por cualquier conducta fuera del recinto escolar durante las horas que no hay clases que represente una amenaza o peligro para la seguridad de los estudiantes, personal, o propiedad del distrito, o sustancialmente interrumpa las actividades de la escuela.

Denegación de responsabilidad

El distrito no hace garantías y niega cualquier responsabilidad por la exactitud o calidad de la información obtenida usando los recursos tecnológicos del distrito. Cualquier declaración accesible por medio de los recursos del distrito se entiende ser el punto de vista del autor individual y no del distrito, sus afiliados, o empleados. El estudiante y padre/madre/tutor, como condición del uso de los recursos tecnológicos del distrito del estudiante, está de acuerdo en indemnizar y librar de cualquier responsabilidad al distrito o a cualquier empleado del distrito y renunciar a todos los reclamos o proceso judicial por daños, costos, o perjuicio surgiendo de la falla de cualquier medida de protección tecnológica, violaciones de restricciones con derechos reservados, errores del usuario o negligencia, u otras obligaciones surgiendo del uso de los recursos tecnológicos del distrito. Cualquier cargo que el usuario acumule debido al uso inapropiado y no autorizado de los recursos del distrito debe ser sostenido por el usuario.

**BAKERSFIELD CITY SCHOOL DISTRICT:
ACUERDO DEL USO ACEPTABLE
ACUERDOS ADICIONALES DEL DISTRITO**

Seguridad y responsabilidad personal

1. Usaré las computadoras de la escuela sin peligro, responsablemente, y para propósitos educativos.
2. Cuidaré la computadora y todo el equipo de tecnología como si me perteneciera.
3. Mantendré mis contraseñas privadas y no las compartiré con mis amigos.
4. Sólo usaré las computadoras de la escuela para el trabajo del salón de clases asignado por el maestro.
5. Reportaré cualquier mal uso de la computadora o red informática al maestro o al director.
6. Me detendré inmediatamente y le diré al maestro o persona encargada si pasa cualquier cosa en la computadora o en el Internet que está mal, o me hace sentir incómodo.

Usos inapropiados

7. No usaré el nombre de usuario y contraseña de alguien más para entrar a la computadora o red informática.
8. No leeré, borraré, copiaré, o modificaré el correo electrónico o usaré otra identidad de la persona.
9. No intentaré pasar sobre las medidas de seguridad en la red informática del distrito.
10. No bajaré ningún software del Internet a menos que se especifique directamente como parte de la lección.
11. No compraré, venderé, o anunciaré cualquier cosa usando la computadora de la escuela y/o red informática.
12. No usaré el equipo de tecnología para animar el uso de drogas, alcohol, y tabaco o tomar alguna acción que sea poco ética o prohibido por la ley o norma del distrito.

Civismo digital

13. No amenazaré, acosaré, insultaré, burlaré, chismearé, o fastidiaré a otros mientras estoy en línea o usando una computadora. Entiendo que estos comportamientos pueden resultar en castigo que incluye la pérdida de privilegios.
14. No copiaré información y la usaré como si fueran mis propias ideas sin darle crédito al autor de la información y fuente. Sé que la falla de citar apropiadamente mis fuentes de información se le llama plagio y es una forma de hacer trampa.

Comportamiento en línea

15. Entiendo que los archivos de la computadora y comunicaciones electrónicas no son privadas y se puede conseguir acceso por el distrito para asegurar el uso propio.
16. No compartiré información personal (ya sea la mía propia ni de otro estudiante) incluyendo: referencias de donde yo vivo, detalles acerca de la familia o amigos (incluyendo nombres), mi edad, cumpleaños, domicilio, o número de teléfono en el Internet.
17. Usaré un lenguaje respetuoso y apropiado sin decir groserías, insultos, o causar a otros que se sientan incómodos debido a su género, raza, apariencia, comportamiento, o creencias. (Estas son acciones que podrían ser consideradas acoso o intimidación).
18. No publicaré material con derechos reservados en línea.

Firmas requeridas: Acuerdo del uso aceptable del BCSD**ESTUDIANTE**

Firmando abajo, estoy mostrando que entiendo y estoy de acuerdo en seguir las reglas escritas en este *Acuerdo del uso aceptable* de cuatro páginas. Entiendo que cualquier regla que no siga puede resultar en acción disciplinaria, perder mi cuenta de usuario, y acción legal. Entiendo aún más que puedo ser responsable por usar los recursos tecnológicos fuera de la escuela si mi conducta viola las reglas del distrito. Estoy de acuerdo en reportar cualquier mal uso del sistema electrónico del distrito a un maestro, director, u otro empleado del distrito.

Nombre del estudiante (escribir con letra de molde): _____

Firma del estudiante _____ Fecha _____

PADRE/MADRE O TUTOR

Como el padre/madre/tutor del estudiante, he leído y entiendo este *Acuerdo del uso aceptable (AUA)* consistiendo de cuatro páginas. Entiendo que este *AUA* ha sido diseñado para ayudar a asegurar una conducta segura y apropiada mientras que el personal y estudiantes usan los recursos tecnológicos. Firmando abajo, yo consiento a que mi estudiante utilice los recursos tecnológicos del distrito consistente con todas las provisiones de este *AUA*. Entiendo aún más que puedo revocar este consentimiento por escrito, pero esta revocación no afectará ninguna acción tomada en virtud de mi consentimiento antes de que el distrito reciba mi aviso de revocación escrito.

Nombre del padre/madre o tutor (escribir con letra de molde): _____

Firma _____ Fecha _____

MAESTRO PATROCINADOR

He recibido y leído la Norma de la Mesa Directiva 400.43 titulada Uso de tecnología del estudiante, la Adjunta Regla Administrativa, y este *Acuerdo del uso aceptable (AUA)* describiendo expectativas para el uso apropiado de los recursos tecnológicos del distrito. Me han proveído con información acerca de la función del personal de supervisar el uso de recursos tecnológicos del estudiante. Como el maestro patrocinador, estoy de acuerdo en instruir al estudiante de cumplir con los requisitos de la norma y del *AUA*. Este compromiso incluye el estar de acuerdo en reportar cualquier uso prohibido o mal uso de los recursos tecnológicos del distrito al administrador apropiado del Distrito Escolar de la Ciudad de Bakersfield y cumplir con todas las leyes, normas, y procedimientos aplicables.

Nombre del maestro/a (escribir con letra de molde): _____

Firma _____ Fecha _____



Name(s)

Class

Date

Directions

When connecting with people online, the Internet opens up many opportunities. However, online communication also has its pitfalls. Fill out the chart below to show the positive and negative online experiences that Randy, Aseal, and Renee describe in the video.

Name	Opportunities (potential positives)	Pitfalls (potential negatives)
<p>Randy <i>Social network sites (Facebook)</i></p>		
<p>Aseal <i>Gaming</i></p>		
<p>Renee <i>Texting and video chatting (Skype)</i></p>		



Name(s)

Class

Date

Internet Safety Tips

If you develop a friendship with someone online, be sure to ask yourself the following questions:

- *Has this person asked me to keep any information secret?*
- *Has this person flirted with me, or asked me about anything sexual?*
- *Has this person asked me about anything private?*
- *Have I felt pressured by this person to do anything?*
- *Do I feel true to myself— sticking to my values — when I talk to this person?*

If someone starts chatting with you about inappropriate topics or asks you to send a picture of yourself, end the conversation immediately. And never plan a face-to-face meeting with someone you met online without taking a parent or guardian along.

Directions

When people drive, they should know the rules of the road. Traffic lights tell them when it's safe to move forward, and when they need to stop.

1. Take three sheets of paper and draw a circle on each one. Color your circle “lights” green, yellow, and red.
2. With your group, read through each of the following stories. Use the Internet Traffic Light descriptions on the next page to help you decide whether it is a green, yellow, or red light situation. When you have made your choice, take one of your lights and place it face down in front of you.
3. Wait until all group members have made their choices, and then flip your papers over. Discuss the choices you made, and decide as a group which one is best.
4. After each story, write down the choice your group made and why.



Stop! Too dangerous to proceed.	The person you are talking to is clearly acting inappropriately, and the conversation needs to end.
Slow down, be cautious – and be prepared to stop.	Something about this conversation makes you feel uncomfortable. You're alert for any signs of inappropriate or suspicious behavior.
Coast is clear (but look both ways!)	You feel safe and enjoy interacting with this person online. But you also remember that all conversations can take unexpected turns, so you're prepared to put the brakes on if you need to. You have not provided any private information.

Abby's Story

Abby is 14. Yesterday was her friend Ivan's bar mitzvah, and Abby chatted with some of his relatives at the party. Today, Abby logs on to the social networking site MyFace and sees a friend request from Ivan's uncle. She doesn't know him very well, but they did chat a little bit about school at the dessert buffet.

What light do you think Abby should choose in this situation? Explain your choice.

Vince's Story

Vince is 12 and loves playing EscapeGo – a fantasy combat MMORPG (massive multiplayer online role-playing game). When he first started playing, another avatar was nice to him and helped him learn the ways of the game. Since then they've been good friends online, completing quests together and protecting each other during combat. Once, one of their teammates asked them how old they were during a quest. "Enough small talk, dude. Nobody cares, just play the game," Vince's friend said in response.

What light do you think Vince should choose in this situation? Explain your choice.



Keyanna’s Story

Keyanna is 13 and she often plays Whatville, a virtual world for middle school kids like herself. One day, another avatar throws a heart her way. Keyanna knows that throwing hearts is a common way to flirt on Whatville. She also knows he’s not a newbie, because it takes someone with a lot experience to design the kind of appearance that his avatar has.

What light do you think Keyanna should choose in this situation? Explain your choice.

Catherine’s Story, Part 1

Catherine, who is 15, logs on to a chat room for teenagers. Her screen name is CathyKisses15. A guy called MikeyMike99 said hi to her a few days ago, and they’ve talked every day since. He’s really easy to chat with, and she likes venting to him about things that annoy her at school and at home. She hasn’t told him anything too personal yet. “U seem so mature. Ur 15 right? I’m 20,” MikeyMike99 says.

What light do you think Catherine should choose in this situation? Explain your choice.

Catherine’s Story, Part 2

Catherine is back online with MikeyMike99, and they’ve been talking for about a week now. He’s starting to flirt with her, and she’s flattered because he seems pretty mature. After all, Catherine’s not really into any of the guys at her school, so she likes flirting with Mike online. She’s pretty good at it too. And yeah, he said something that might have been kind of sexual once or twice. Today he writes, “Can I show u a pic?” Before she types a response, he says again: “Keep this private ok? I like u, Cat. I hope u like me 2.”

Now what light do you think Catherine should choose? Explain your choice.



Name(s)**Class****Date**

Directions

Read the tips below on how to make and use strong passwords. Then read stories about Jessie and Krystal and answer questions about their passwords. Use the tips to make new passwords for Jesse and Krystal.

DO'S

- **DO** share your password only with your parents.
- **DO** create passwords with at least eight characters.
- **DO** use combinations of letters, numbers, and symbols, which are harder to crack than just words.
- **DO** change your password regularly – at least every six months.

DON'T'S

- **DON'T** give a password to anyone else – not even your friends.
- **DON'T** use passwords that are easy for people you know to guess, like your nickname or your pet's name.
- **DON'T** use any private identity information in your password.
- **DON'T** use a word in the dictionary as a password.

Use Common Sense!

Know what the kinds of private identity information not to include in your password:

- Full (first and last) name
- Email address
- Passwords
- Credit card numbers
- Mother's maiden name
- Postal address
- Phone numbers
- Calling card numbers
- Social Security number



Smart Passwords?

Directions

Read the following stories and answer the questions.

Jesse lives in Lawrence, Kansas – the home of the University of Kansas. He has a pet rat named “Phil” and is a big fan of the Kansas Jayhawks men’s basketball team. Jesse chose “jayhawks” as his password. Did he make a safe choice? Why or why not?

Krystal lives in Miami, Florida. Her birthday is August 4, and she swims on a team. Her password is “krswim84.” How did Krystal choose her password? Was it a safe choice? Why or why not?

You Try It!

Directions

Using the tips above, make new passwords for Jesse and Krystal. Explain how Jesse and Krystal can remember their passwords.

Jesse _____

Krystal _____



Name(s) _____

Class _____

Date _____

Directions

You will create one strong and one weak password for an important historical figure. Both passwords should indicate something that is special or unique about that person. Use the “Do” tips from the **Password Tips Student Handout** to create the strong password, and use the “Don’t” tips from the same handout to create the weak password.

Example for Abraham Lincoln:

Strong: 4score7yrs (“Four Score and Seven Years Ago ...”)

Weak: HonestAbe

YOUR HISTORICAL FIGURE: _____

FACTS OR INFORMATION YOU LEARNED ABOUT YOUR HISTORICAL FIGURE: _____

STRONG PASSWORD: _____

WEAK PASSWORD: _____

Directions

Place check marks in all of the boxes that describe your answers to the questions below.

1. How did you come up with your strong password? What strategies did you use?

- I chose something that was connected with my person, but not too obvious.
- I replaced certain letters with numbers and symbols.
- I abbreviated words.
- Other: _____



2. What makes your weak password less secure than the strong one?

- I didn't use any numbers.
- I used whole words that were commonly associated with my person.
- I used the person's name or an obvious nickname.
- Other: _____

3. How could the weak password be more secure without changing it a lot?

- Abbreviate words.
- Replace letters with numbers/symbols.
- Spell out words in number form (A-1, B-2, C-3, D-4 ...).
- Other: _____