Hoy en día, vivimos en una sociedad que se denomina “sociedad digital” y nuestro alumnado ha nacido con el calificativo de “nativos digitales”. Una “nueva cultura” nos rodea donde la protagonista es la Tecnología de la Información y de la Comunicación (en adelante TIC) y su uso, sobre todo desde la pandemia, va en aumento. El uso de la TIC tiene que ir unido a una concienciación del alumnado para ser ciudadanos digitales ejemplares.

Como centro educativo debemos proponernos no sólo desarrollar y llevar a cabo contenidos de nuestras materias, sino tratar este tema transversal en los trabajos, proyectos, investigaciones, presentaciones o infografías que realizan nuestros alumnos relacionados con las diferentes asignaturas.

La seguridad en línea o digital en el IES Rusadir conlleva detenernos en explicar y tener en cuenta las siguientes consideraciones:

1. Netiqueta – la buena educación (también debe estar presente) en redes e internet. Códigos de conducta en las plataformas digitales.

2. Acoso digital o Ciberacoso.

3. Derechos y obligaciones en la red. Intimidad, privacidad y protección de datos.

4. Derechos de autor.

5. Protección contra el malware en el centro.

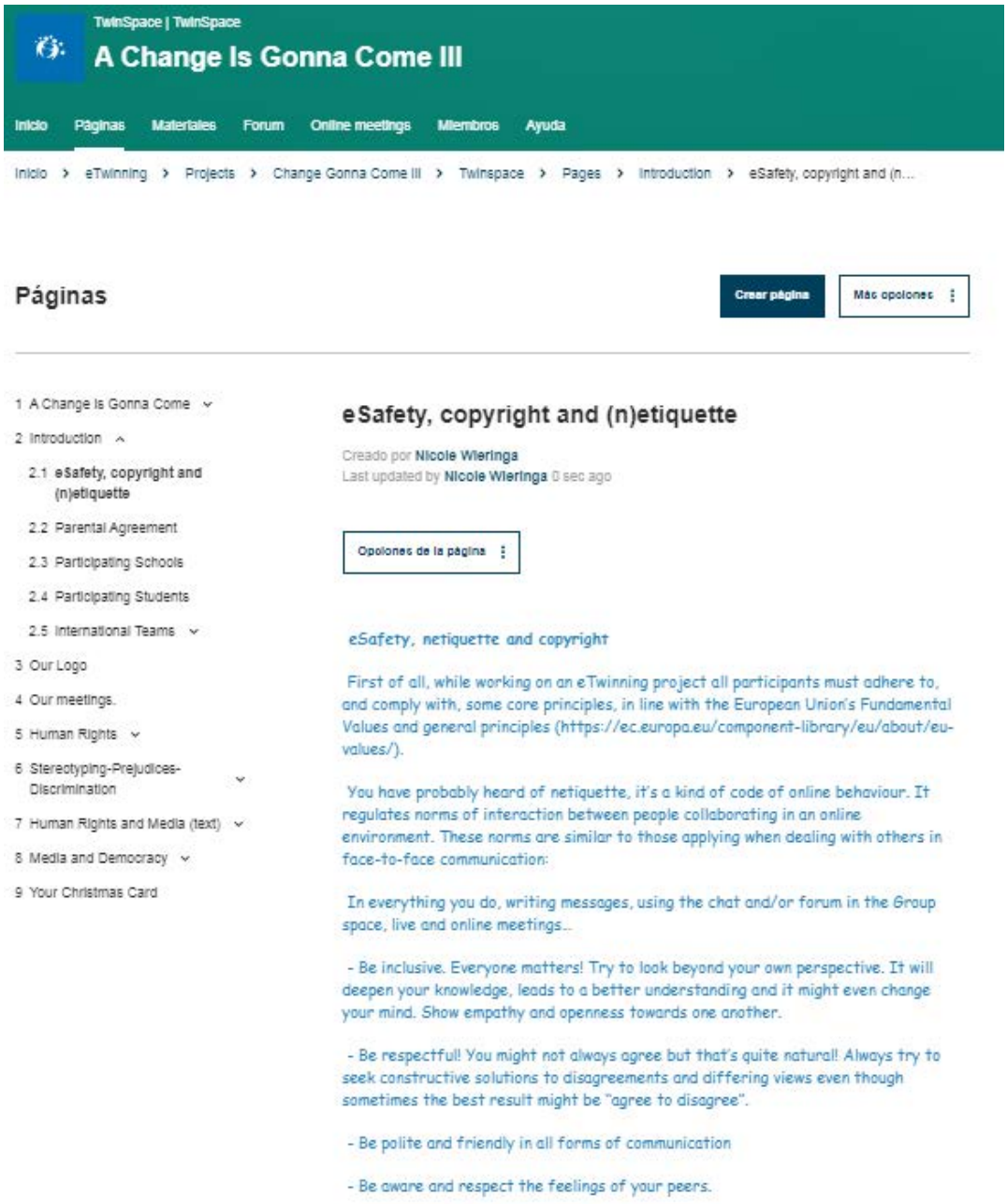
6. Protección de datos confidenciales en el centro.

Todas las consideraciones nombradas anteriormente tienen que conocerse entre el profesorado y las familias, con el fin de concienciar desde todos los ámbitos a nuestros jóvenes para un uso razonable y responsable de las TIC así como, un comportamiento disciplinado en la red.

1. Netiqueta

Este punto se desarrolla en las materias del departamento de Tecnología, durante las sesiones de tutoría y charlas de la Policía Nacional (Plan Director) pues forma parte del Plan de Acción tutorial de nuestro centro. En las sesiones con el alumnado se tiene en cuenta:

I. Presentaciones, textos y enlaces alojados en proyectos eTwinning : e-safety



II. Enlaces donde se trata el comportamiento adecuado en comunidades digitales:

eTwinning

Facebook

Youtube

Twitter

Instagram

Snapchat

Sé genial en Internet- Google PARA JÓVENES / EDUCADORES / FAMILIAS

III. Página web del centro donde se publican estos contenidos:

Seguridad en línea- eSafety en el IES Rusadir

Asimismo, se trata el tema en la materia de Tecnología tanto en secundaria como en Bachillerato.

2. Acoso digital o Ciberacoso.

Considerando que el ciberacoso pertenece al punto de acoso escolar, una vez detectado y confirmado algún caso de acoso digital en nuestro centro, será tratado atendiendo al protocolo de actuación ante situaciones de acoso escolar en los centros docentes públicos no universitarios.

Con el fin de evitar el acoso escolar entre nuestro alumnado, este tema es tratado en las sesiones de tutoría y en las charlas recibidas por agentes de la policía nacional con el alumnado de todos los niveles. Las actuaciones señaladas forman parte del Plan de Acción Tutorial del centro.

3. Derechos y obligaciones en la red. Intimidad, privacidad y protección de datos.

La red internet es un mundo muy extenso, complejo, útil pero a la vez peligroso para nuestros jóvenes si no hay concienciación en cuanto a un uso correcto, disciplinado y racional así como, llevar a cabo las pasos adecuados para mantener una adecuada privacidad y protección de datos en esta enorme telaraña de información. Es por ello, que nuestros alumnos deben ser conocedores de cómo proceder para garantizar su intimidad en la red. Para desarrollar este punto y como punto de ayuda en las sesiones de tutoría y de las materias T.I.C. se trabajarán actividades sobre e-safety al comienzo de todo proyecto e-Twinning que tenga lugar en nuestro centro.

También es importante tener en cuenta las recomendaciones publicadas en la página de la Unión Europea en cuanto a la protección de datos de menores de edad.

https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_es.htm#shortcut-3

4. Derechos de autor.

Los derechos de autor son un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley reconoce a los autores de una obra publicada. La propiedad intelectual agrupa todos los derechos del autor sobre la disposición y explotación de su creación.

Los sitios web, comerciales o no, están compuestos por contenidos digitales como textos, fotografías, vídeos, animaciones, música, software etc. y todos ellos, sean nuestros o de terceros, están sujetos a una serie de limitaciones. Es decir, su utilización viene definida por la licencia elegida por su autor para aplicarla a cada contenido publicado. Veamos las licencias más habituales para estos ítems:

• Copyright (©). Esto indica que la obra o recurso con esta licencia establecida no se debería emplear, si no es con el consentimiento expreso del autor.

• Creative Commons (CC), GPL .Licencia de tipo abierto generalmente el material se puede emplear, incorporar, modificar y difundir; pero siempre debemos ceñirnos a lo que se indique en la licencia: si se nos indica aspectos como que debemos citar la autoría o si no podemos hacer modificaciones. No requiere pedir consentimiento, sólo seguir las pautas indicadas.

Si en el material no hay nada indicado o no es posible localizar su fuente, sería mejor no emplearlo, ya que podríamos encontrarnos con que su autor nos reclame su reconocimiento de autoría en un futuro.

Por tanto, la mejor recomendación para reutilizar contenidos es la de incorporar exclusivamente materiales con licencias abiertas, como Creative Commons. En Internet encontraremos múltiples espacios web donde localizar recursos que podemos emplear.

En cuanto a los tipos de licencias relativos a programas o aplicaciones que usamos en las aulas, podemos nombrar:

- Software comercial.
- Shareware.
- Freeware.
- Software libre.

5. Protección contra el malware en el centro.

La protección contra el malware en nuestro centro se lleva a cabo con la puesta en marcha de las siguientes acciones:

• Instalación de sistemas hardware de protección con cortafuegos en la red principal del centro.

• Instalación de sistemas antivirus en los ordenadores de administración del centro.

• Congelación con el software adecuado los equipos informáticos que son usados por el alumnado en las aulas.

• Bloqueo de sitios web y ventanas emergentes no deseados personalizando la configuración de seguridad del/de los navegador(es) que se utilizan en los ordenadores del centro.

6. Protección de datos confidenciales en el centro.

Este apartado se desarrolla con las siguientes actuaciones:

• Establecimiento dos redes, una cableada y otra wifi. La red Ethernet se subdivide en alumnado, profesorado y administración. La red wifi se subdivide en alumnado, profesorado e invitado.

• Realización de copias de seguridad de los dispositivos necesarios con regularidad.

• Configuración adecuada de sistemas software de protección cortafuegos y antivirus.

Por lo que respecta al resto de apartados de este punto cumplimos estrictamente lo dictado en la Ley de Protección de datos personales y garantía de derechos digitales.

https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf