ESAFETYLABEL.EU eSafety certified For a safer school !

eSafety Label - Action Plan for: Collège Paul Gauguin

Assessment form was submitted by: Maxime Drouet - 2015-02-06 09:43:31

By submitting your completed Assessment Form to the eSafety Label portal you have taken an important step towards analysing the status of eSafety in your school. Congratulations! Please read through your Action Plan carefully to see what you can do to improve eSafety further in your school. The Action Plan offers useful advice and comments, broken down into 3 key areas: infrastructure, policy and practice.

Infrastructure

Technical security

- You have some filtering in your school. Consider whether some differentiated filtering is needed depending on the ages and needs of different pupils. If there are lots of incidences of users accessing inappropriate content then it may be worth considering whether additional filtering or additional education (or both) are needed.
  An educational approach and building resilience in pupils of all ages is also key to safe and responsible online use so bring together all teachers to have a discussion on how they will talk to their pupils about being a good and safe digital citizen. See www.paneuyouth.eu for examples of discussions that can take place in the classroom on this topic, through role-play and group games.
- Your school system is protected by a firewall. Ensure that the provision and management of the firewall are regularly reviewed and updated, as and when required.

Pupil and staff access to technology

- You need to provide different WiFi networks for different purposes within the school, e.g. a secure network for staff /core business, a guest network for visitors and casual use.
  Staff and pupil use of their own equipment on the school network needs to be addressed in an Acceptable Use Policy so that users are clear about which networks they should use and why. Your Acceptable Use Policy needs to include clear guidance about which activities are permitted while on the school network, and what is not allowed.
- Consider whether banning mobile devices is a rule that is fit for purpose and if your school might want to allow digital devices for some class activities. You could develop as part of your Acceptable Use Policy a section on how digital technologies can and cannot be used in the classroom; see the fact sheet on *Using Mobile Phones at School* (www.esafetylabel.eu/group/teacher/mobile-phones).

Data protection

- It is good that all users are attributed a different password by the system in your school. Remind all school members never to write their given password down anywhere, certainly not on a sticker on a computer! Also, ensure that the Acceptable Use Policy reminds staff and pupils to keep their passwords secure and not share them with others.
- Any data relating to pupils should be encrypted before it is sent or stored electronically. Investigate urgently how data can be protected, making use of other school's advisers or good practice guides, and take action. See the fact sheet on *Protecting Sensitive Data* (www.esafetylabel.eu/group/teacher/protecting-sensitive-data).

Software licensing

- You need to make sure that all the software in your school is legally licensed and that copies of the licences are held centrally. You also need to check with whoever supports your IT systems that the software will not compromise system security. Your school should develop a clear policy for software acquisition and it is good practice to centralise this process wherever possible.
- Ensure that all staff are aware of the procedure for purchasing new software and that all licenses are appropriate for the number of pupils and staff that will be using them. The End-user license agreement section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

IT Management

- It is good practice to have a centrally organized system for patch management. Could you ask your ICT systems manager to create a short tutorial on patch management for upload to your school profile? This will be very helpful for other schools.
- In your school only the head master and/or IT responsible can acquire new software. Consider putting a system into place where teachers can ask for new software in a non-bureaucratic and timely fashion. This allows teachers to create a more engaging lesson without the temptation of unauthorized copying and its inherent dangers and costs.

Policy

Acceptable Use Policy (AUP)

- Your school should consider all policies which can refer to eSafety issues and the eSafety policy (such as child protection, safeguarding, behaviour). When drawing up school policies, keep in mind that online activities can have an impact on all areas of pupil and staff activities. Refer to eSafety aspects too, for example in child protection and anti-bullying policies, and ensure that your various policies are coherent with each other.
- Work with all stakeholders in your school to develop a section in your School Policy and your Acceptable Use Policy to include information on mobile phone usage in the school. Ensure that this is communicated to all staff and consistently enforced. The fact sheets on *Using mobile phones at school* (www.esafetylabel.eu/group/teacher/mobile-phones) and *School Policy* (www.esafetylabel.eu/group/teacher/school-policy) will provide helpful information.

Reporting and Incident-Handling

- There needs to be a clear procedure for dealing with material that could potentially be illegal which takes into account law enforcement issues. There should be a named person from the school senior leadership team who takes overall responsibility in this type of case, and the procedure needs to be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Remember to report any suspected illegal content to your national INHOPE hotline (www.inhope.org).
- Draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines.

Staff policy

- There are dangers associated with the use of personal mobile devices in class. Consider why staff would need to use their device and, if appropriate, consider providing a school device. Advise staff to read the fact sheet on *Using mobile phones at school* (www.esafetylabel.eu/group/teacher/mobile-phones) and ensure that the guidelines to staff are clearly communicated in the School Policy.
- New technologies, such as smartphones or other mobile devices bring a new set of risks with them. Ensure that your teachers are aware of those. This way they can avoid the pitfalls when using the devices and also pass the knowledge onto the pupils.

Pupil practice/behaviour

- Electronic communication guidelines for pupils should be clearly communicated in the Acceptable Use Policy.

Communication between pupils can rapidly degenerate if standards are not set, giving rise to incidents such as cyberbullying. Learning about effective, responsible communication should also be part of the school curriculum, as it is a necessary competence for every young person. Discuss this at a staff meeting in order to define the standards you want to implement.

- A hierarchy of positive and negative consequences should be applied to all on- and offline issues. It should be clearly communicated to all members of the school community and all stakeholders should be involved in drawing up and agreeing the consequences.

School presence online

- It is important that the ICT coordinator has an overview of any social networking profiles set up by representatives of your school. Check the fact sheet on *Schools on social networks*(www.esafetylabel.eu/group/teacher/social-networks) for further information to make sure that good practice guidelines have been followed. Consider setting up a school social media profile to facilitate monitoring and showcase initiatives and achievements, as this can be a useful dissemination tool.
- It is good that pupils can give feedback on the school's online presence. Think about creating a space that is entirely managed by pupils. It's a great opportunity to learn about media literacy and related issues. It also can help to establish a peer network of support. Find out more about in the eSafety Label fact sheet.

Practice

Management of eSafety

- Consider appointing a governor or board member who provides a liaison for eSafety issues. Consider also reporting on the number and type of eSafety incidents to the governing body on an annual basis when you also review your School Policy. See our fact sheet on *School Policy* www.esafetylabel.eu/group/teacher/school-policy.
- Appoint a person who will have overall responsibility for eSafety issues. Ideally this should be someone from the senior leadership team. Ensure that this person is involved in the development and regular review of your School Policy. She or he should not only be informed, but should also fill out the *Incident handling form* whenever an incident arises at www.esafetylabel.eu/group/teacher/incident-handling.

eSafety in the curriculum

- Ensure that the eSafety curriculum keeps up with emerging issues by making full use of all available resources and ensure that it builds on prior learning, bearing in mind that pupils will need different messages depending on how they are using the technology.
- It is important that children understand the responsibilities and consequences when using social media (e.g. Facebook, Blogs, Instagram, Google+, etc). See with your teachers how this could be integrated into the lessons. Topics would include digital footprint, data privacy.

Extra curricular activities

- Try to engage pupils in peer mentoring and provide them with opportunities to share their thoughts and understanding with their peers. Also check out the resource section of the eSafety Label portal to get further ideas and resources.
- Consider carrying out a simple survey in order to establish what pupils are doing when they go online. This will help to inform eSafety education within the school. Share your survey questionnaire and results in the eSafety Label community via your My school area (avoiding publishing any personal information) so that other schools can benefit from your work and even share their results with you for comparative purposes.

Sources of support

- Consider providing eSafety information for parents through the school website or by providing links in a school newsletter. It may be possible to run a parent information evening. See the fact sheet *Information for parents* at www.esafetylabel.eu/group/teacher/info-for-parents to find resources that could be circulated to parents and ideas for parent evenings.

- Young people are more open to advice from their peers. Consider offering facultative courses and/or school rewards on eSafety topics or similar that stimulate expert knowledge in pupils that then could become a point of reference for their peers.

Staff training

- All teachers should be able to recognise signs of cyberbullying and be aware on how to best proceed. Make sure that your teachers are regularly trained bearing in mind the rapid changes of new technology. Also check the eSafety fact sheet on *Cyberbullying* at www.esafetylabel.eu/group/teacher/cyberbullying.
- Consider ways to facilitate knowledge exchange between staff members. This could be in form of an online community with a platform, an email exchange or within a frame of staff initiated meetings. A school in which all staff members are aware of eSafety related issues is a much safer school. Suggest eSafety related topics for these sessions.

The Assessment Form you submitted is generated from a large pool of questions. It is also useful for us to know if you are improving eSafety in areas not mentioned in the questionnaire. You can upload evidence of such changes via the Upload evidence on the My school area section of the eSafety Portal. Remember, the completion of the Assessment Form is just one part of the Accreditation Process, because the upload of evidence, your exchanges with others via the Forum, and your reporting of incidents on the template provided are all also taken into account.