



eSafety Label - Action Plan for: Sint Michael College

Assessment form was submitted by: Dennis Jurhill - 2015-06-15 14:43:41

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

- Although asking users to define their own filtering is a good way to encourage responsible use, most school-aged pupils are not mature enough to make an informed decision about the level of filtering they should be using. The school, or at the very least the teacher, needs to decide on what level of filtering is used. This can be done after discussion with the class to make them aware of the reasons for any filter that is installed. Pupils' parents would typically prefer that filtering is set by the school or teacher as young people are often not aware of what they could come across by accident, whether potentially harmful or illegal. However, 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.
- It is good practise that your IT services are regularly reviewed, updated and removed if no longer in use.

Pupil and staff access to technology

- Ensure that the policy on mobile phones is being applied consistently throughout the school. Take a look at the fact sheet on *Using Mobile Phones at School* (www.esafetylevel.eu/group/teacher/mobile-phones).
- It is great that in your school laptops/tablets are easily accessible within a lesson. Using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.

Data protection

- Your new users are given a standard password and are asked to generate their own password on their first access. Passwords offer unique entry points into the school computing system and some basic rules of password security should be rigorously applied. For further information, read the fact sheet on *Safe passwords* at www.esafetylevel.eu/group/teacher/safe-passwords. Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.
- It is good that your school provides materials on the importance of protecting devices, especially portable ones. Ensure that staff are aware of these and use them. This material should be pointed out to new staff as part of their induction. Please consider sharing those with others through the in . Also ensure that your materials are regularly reviewed to ensure they are in line with the state of the latest technology.

Software licensing

- 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.
- Your school has set a realistic budget for software needs. This is good. Ensure that it remains this way. You might also want to look into alternatives, e.g. Cloud services or open software.

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.
- It is good that staff members with questions about software issues can contact a school helpdesk. Consider whether you need to provide training and/or guidance to new software that is installed on school computers. This is important to ensure that school members will take advantage of new features, but also that they are aware of relevant security and data protection issues.

Policy

Acceptable Use Policy (AUP)

- It is excellent that eSafety is an integral part of several school policies. Do all staff make reference to it when appropriate through their teaching? Look for examples of good practice and share these with staff and pupils. Produce a short case study to highlight this good practice and upload it to your profile on the eSafety Label portal via your [My school area](#) as inspiration for other schools.
- It is good that school policies are reviewed annually in your school. Ensure that they are also updated when changes are put into place that could affect them. All staff should be aware of the contents of the policy.

Reporting and Incident-Handling

- Ensure that all staff, including new members of staff, are aware of the guidelines concerning what to do if inappropriate or illegal material is discovered on a school machine. Ensure, too, that the policy is rigorously enforced. A member of the school's senior leadership team should monitor this.
- It is good practice to log cyberbullying incidents that occur in your school centrally, as you are contributing to building a data base of successful incident handling practices from schools across Europe that you and others can use in future. Make sure that pupils sign up to anti-bullying guidelines in your Acceptable Use Policy.

Staff policy

- Ensure that all staff understand the school's regulations on use of personal mobile devices in the classroom; these should be clearly communicated in the School Policy. Monitor the effectiveness of the policy and ensure that it is adhered to. You can also advise your staff to read the fact sheet *Using mobile phones at school* (www.esafetylevel.eu/group/teacher/mobile-phones).
- In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.

Pupil practice/behaviour

- You have defined electronic communication guidelines in your Acceptable Use Policy and this would be a useful example of good practice for other schools. Can you create a tutorial about electronic communication guidelines for pupils and upload it to your school profile via your [My school area](#) so that other schools can benefit from your experience.
- Your school partly has a school wide approach of positive and negative consequences for pupil behaviour. This is a good start, make sure that the policy and associated hierarchy applies to all on- and offline issues and is shared widely and re-visited by all staff and pupils at least annually.

School presence online

- Check the fact sheet on *Taking and publishing photos and videos at school* (www.esafetymlabel.eu/group/teacher/photos-videos) to see that your School Policy covers all areas, then upload this section of your School Policy to your profile page via your [My school area](#) so that other schools can learn from your good practice.
- Regularly check the content of the school's online presence on social media sites to ensure that there are no inappropriate comments. Set up a process for keeping the site/page up to date, and check the fact sheet on *Schools on social networks* (www.esafetymlabel.eu/group/teacher/social-networks) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.

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.esafetymlabel.eu/group/teacher/school-policy.
- Technology develops rapidly. Consider sending the ICT responsible regularly to trainings and/or conferences to be aware of new features and risks. Check out the fact sheet .

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 good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

Extra curricular activities

- It is good that you provide eSafety support for your pupils outside curriculum time when asked. Consider offering all pupils support to deal with online safety issues. It may be helpful to provide a "surgery" to help pupils to set their Facebook privacy etc. The eSafety Label portal provides resources that will be useful for this; check out the fact sheet on *Pupils' use of online technology outside school* at www.esafetymlabel.eu/group/teacher/social-media-pupils.
- 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.

Sources of support

- All staff should have some responsibility for eSafety. School counsellors, nurses, etc. are all well placed to provide advice and guidance on these issues and should be invited to contribute to developing and regularly reviewing your School Policy. Make the maximum use of their knowledge and skills and consider whether it is appropriate to provide training for them.
- It is good that you provide eSafety support for parents when asked. Consider providing regular information for all 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.esafetymlabel.eu/group/teacher/info-for-parents to find resources that could be circulated to parents and ideas for parent evenings.

Staff training

- Your school makes sure that every teacher is trained on cyberbullying. Please share resources that are used in

these trainings via uploading them to your [My school area](#). Are you also monitoring the effect that this training had on the number of incidents?

- It is important that teachers are aware on the technology used by pupils in their freetime. This is important as this awareness is the first step in addressing the issue of powering down for school. At the same time pupils should not be asked to do their homework using technology not available to them outside of schools. Ensure that all teachers are provided with information of this. Have a look at the [Essie Survey of ICT in schools](#).

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.