eSafety Label - !action_plan_for! Herskindskole og Børnehus

!assessment_form_submitted_by! Lene Yang - 2015-10-02 12:21:59

!action_plan_intro!

Infrastructure

Technical security

- It is very good that all your school computers are virus-protected. Make sure you also have included a paragraph on virus protection in both your School Policy and your Acceptable Use Policy, and ensure that staff and pupils rigorously apply school guidelines. If you need further information, check out the fact sheet on *Protecting your devices against malware* at www.esafetylabel.eu/group/teacher/protecting-devices-against-malware.
- 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

- All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. Check the fact sheet on *Use of removable devices* at www.esafetylabel.eu/group/teacher/removable-devices to make sure you cover all security aspects.
- 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.esafetylabel.eu/group/teacher/mobile-phones).

Data protection

- You have a good policy of keeping separate your learning and administration environments. It is good to ensure staff training is up-to-date on managing these environments as you continue to review your policies. Share your policy with other eSafety Label by uploading it to your school profile.
- You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data controller for your school. Upload to your school profile some guidelines about protecting sensitive data through an encryption system so that other schools can benefit from your experience.

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.
- It is good practise that the member of staff responsible is fully aware of installed software and their license status.

IT Management

- In the interests of innovative pedagogical practice, it may seem necessary to allow staff and pupils to upload

software to school-owned hardware, however this should only be done by the person in charge of the school ICT network in conformity with the School Policy. Staff and pupils should be aware of this through the Acceptable Use Policy they are required to sign. All new software uploaded to school equipment needs to be in conformity with licensing requirements.

- There is a mechanism set up in your school that allows any staff member to make a request for new hard/software - a request that leads to an informed decision within a reasonable amount of time. This is great as this way teacher can benefit from new technologies while still staying inline with school policy.

Policy

Acceptable Use Policy (AUP)

- It is good that you have an Acceptable Use Policy (AUP) for pupils. You should now amend the AUP to include staff and the wider community. To ensure that your revised AUP is sufficiently comprehensive, take a look at the fact sheet and check list on *Acceptable Use Policy* at www.esafetylabel.eu/group/teacher/acceptable-use-policy.
- 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.

Reporting and Incident-Handling

- Have teachers received training on dealing with potentially illegal material? Is the procedure clearly indicated in the School Policy and the Acceptable Use Policy which all teachers and pupils have signed? All staff and pupils should be aware that they should report any suspected illegal content to the national INHOPE hotline (www.inhope.org).
- It is important to have a clearly communicated School Policy on this, and it should be mentioned in the Acceptable Use Policy too. What is considered to be potentially illegal can vary from person to person, so it is important that this is discussed with staff members and that school standards are set. All members of the school including pupils and teachers must be informed of them and required to respect them.

Staff policy

- There should be a code of conduct for staff so that they are clear about what is acceptable behaviour when they are online. This should be clearly communicated to all staff in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.
- In your school user accounts are adjusted within a weeks delay if the role of staff or pupil changes. Investigate if this process could be optimised. The quicker that unused accounts are deactivated/adjusted, the less risk of misuse.

Pupil practice/behaviour

- Electronic communication guidelines for pupils should be clearly communicated in the Acceptable Use Policy. Communication between pupils can rapidly degenerate if school-wide 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.
- When discussing eSafety pupils at your school can sometimes provide feedback on the activities . Involve them as much as possible so that the teacher recognises real life issues while the pupils are more engaged.

School presence online

- Check the fact sheet on *Taking and publishing photos and videos at school* (www.esafetylabel.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.

- We recommend that you specifically nominate a web-experienced staff member to periodically check the school's online reputation. Monitoring such an important aspect on an ad hoc basis only is insufficient. Remember that this is the image that prospective parents will receive when they search for your school online.

Practice

Management of eSafety

- In your school, teachers are responsible for their own pupils' online activity. There are many network security and user privacy, audit and procedural tool checks and balances that need to take place to ensure the safety of your pupils and the school networks, and these should be laid down in your School Policy. See our fact sheet on *School Policy* at www.esafetylabel.eu/group/teacher/school-policy.
  To ensure this happens as efficiently and often as necessary, we advise that the Principal of your school appoints one individual staff member to look after eSafety management in the school. This person will be responsible for seeing that all aspects included in your School Policy are discussed and looked at with other teachers as well as with pupils in the classroom.
  To ensure that every staff member, pupil and parent is aware of her or his online rights and responsibilities, see the fact sheet on *Acceptable Use Policy* (www.esafetylabel.eu/group/teacher/acceptable-use-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

- eSafety needs to be embedded within the curriculum regardless of whether this is a statutory obligation in your country. There are several very good schemes of work freely available which will support this. For further information see the fact sheet *Embedding eSafety in the curriculum* at www.esafetylabel.eu/group/teacher/esafety-in-curriculum.
- Cyberbullying is the most important issue that helplines are contacted about and can have a devastating effect on pupils' life. Try to discuss this with pupils from a very early age on, maybe in the form of role plays. Also check our fact sheet on for more information.

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.esafetylabel.eu/group/teacher/social-media-pupils.
- 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

- 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.
- 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

- Although staff in your school do not receive training on eSafety, they need to be regularly updated about emerging trends. Consider a needs-analysis to determine what different staff require from their training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.eu/group/teacher/esafety-training-courses.
- In your school knowledge exchange between staff members is encouraged. This is beneficiary to the whole school. Upload powerpoints, documents or similar of knowledge exchanges on eSafety topics to your .

!action_plan_conclusion!