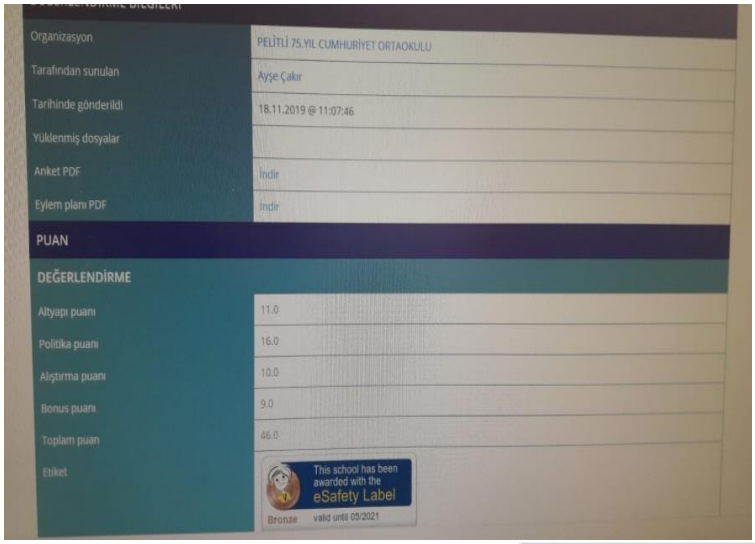
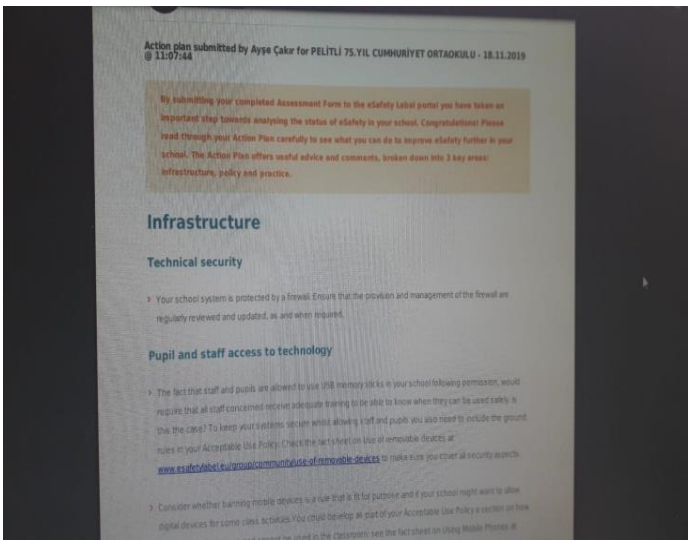
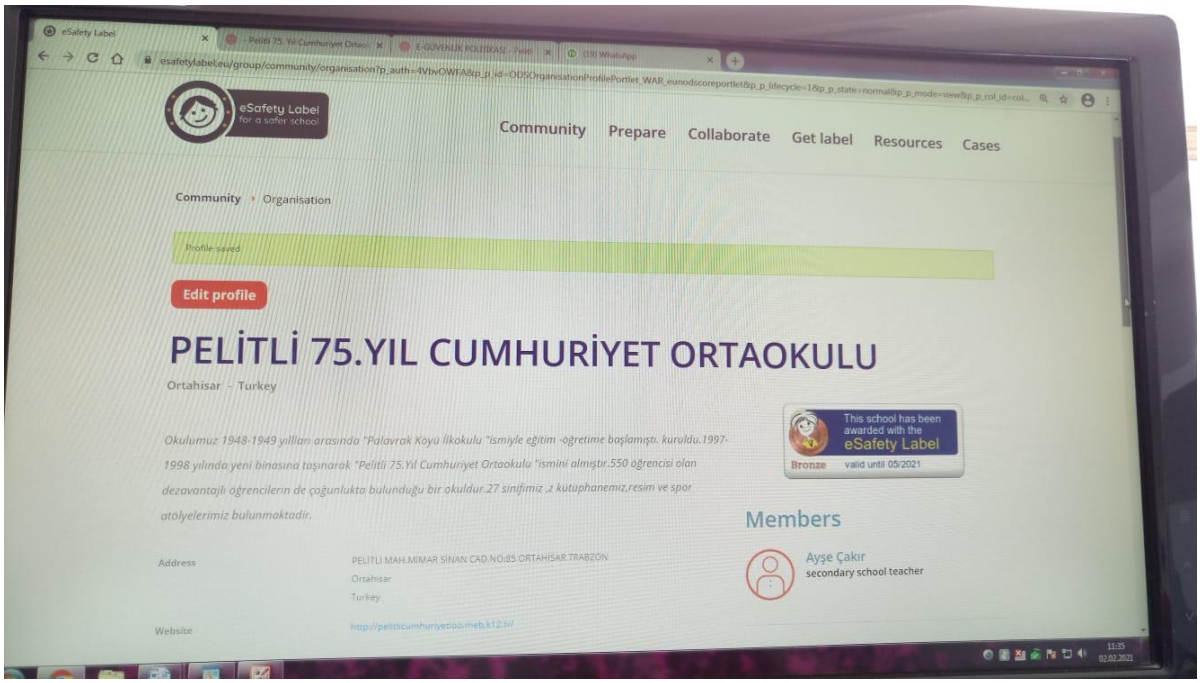
PELİTLİ 75.YIL CUMHURİYET ORTAOKULU

ESAFETY ETİKETİ:18 Kasım 2019 tarihinde yaptığımız başvuru neticesinde bronz etiketimizi aldık. Tekrar eylem planı doğrultusunda eksiklerimizi gidererek gümüş etiket için başvuruyu yaptık.



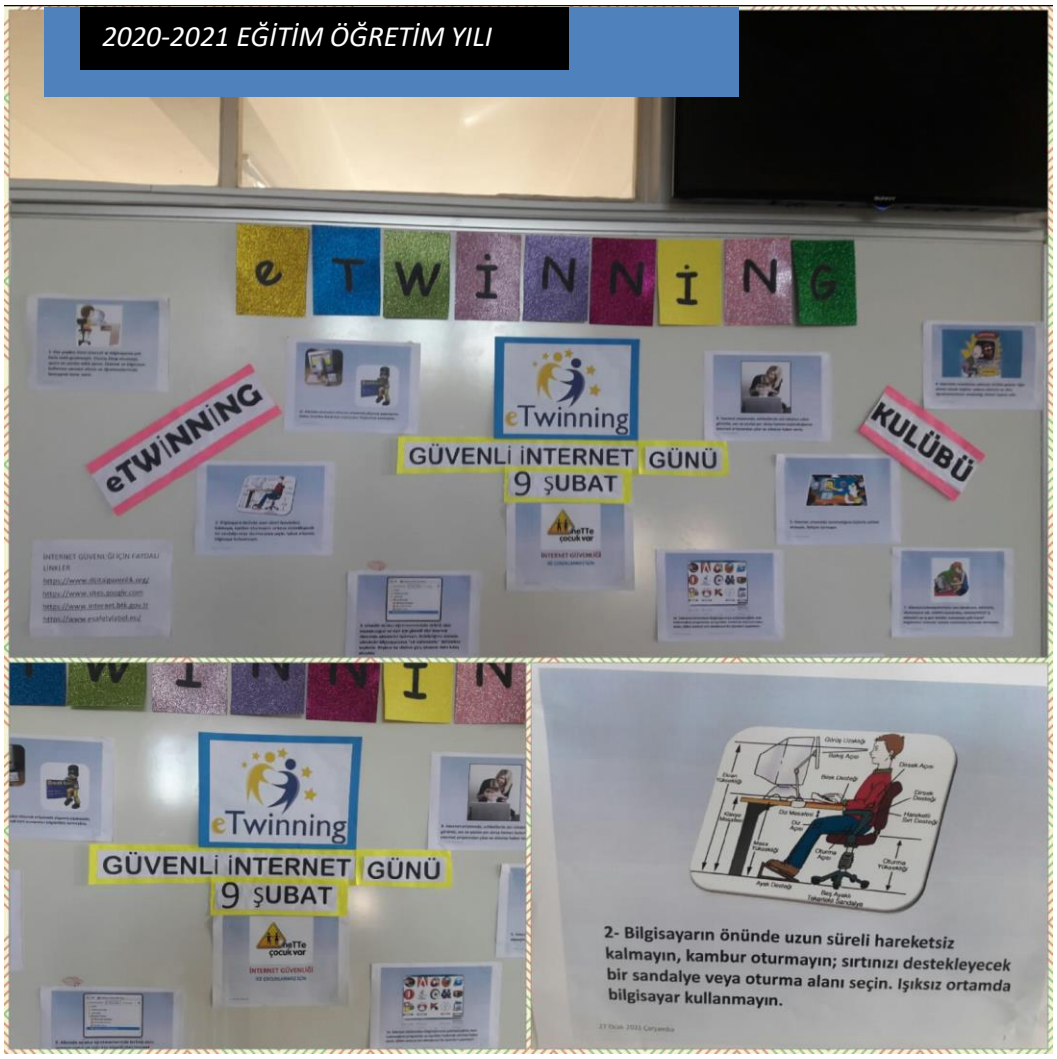




OKUL SİTESİNDE E-GÜVENLİK ÇALIŞMALARI

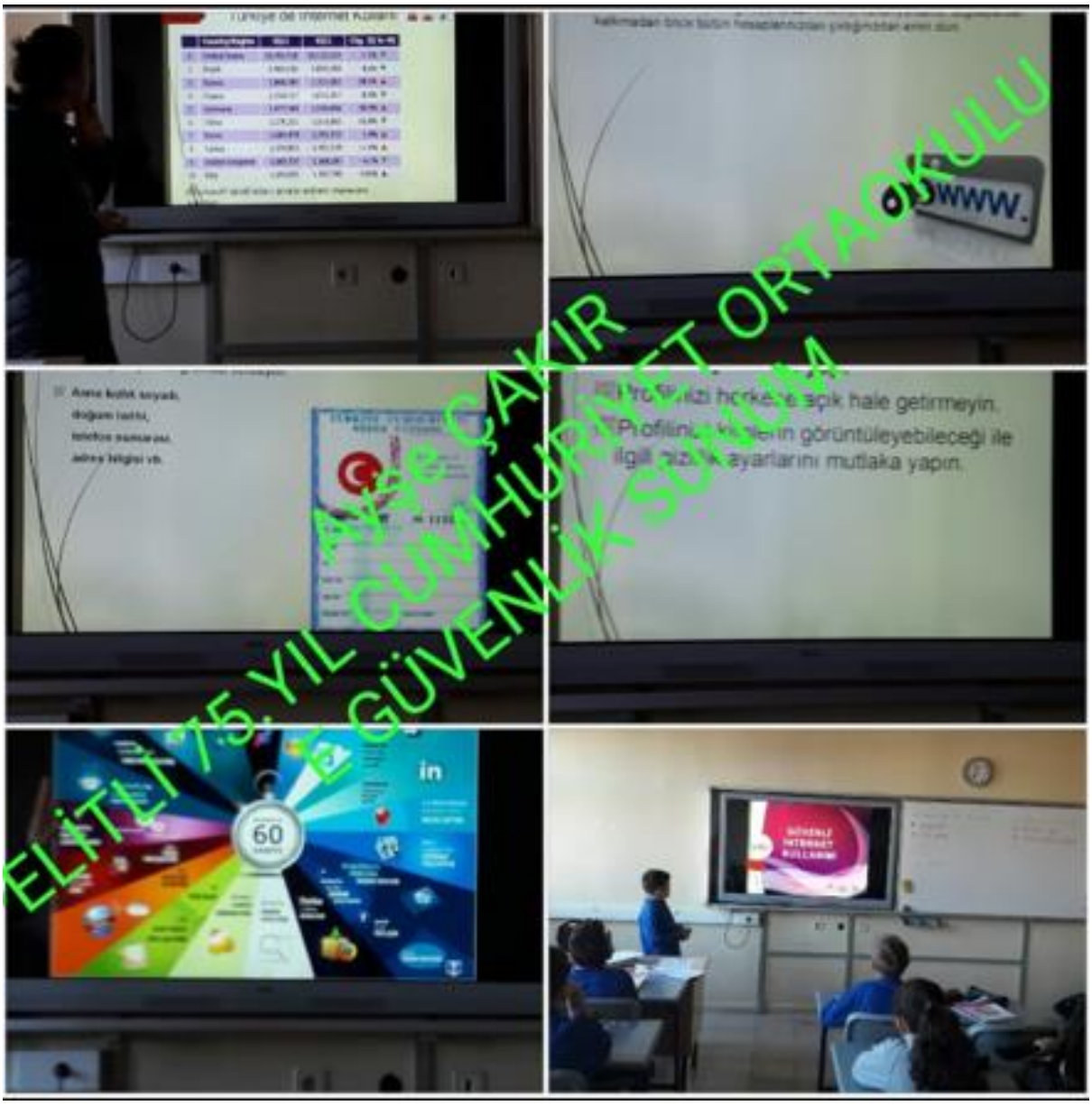
http://pelitlicumhuriyetioo.meb.k12.tr/icerikler/e-guvenlik-politikasi_10390881.html

E-GÜVENLİK İNTERNET PANOLARIMIZ

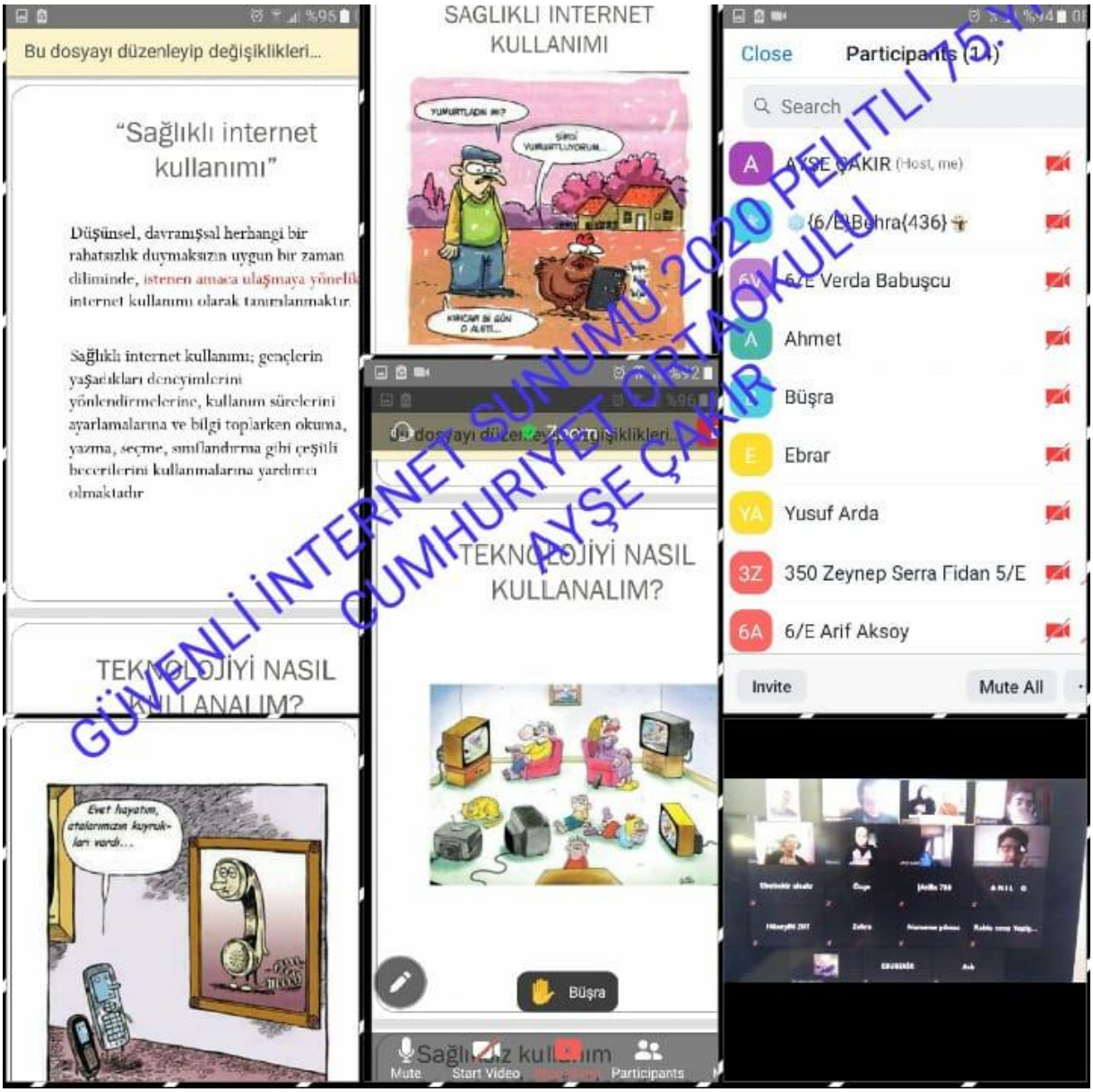


2019-2020 E-GÜVENLİK SUNUMU

2019-2020 E-GÜVENLİK SUNUM



2020-2021 UZAKTAN E-GÜVENLİK İNTERNET SUNUMU



E-GÜVENLİK SERTİFİKALARIMIZ

E-GÜVENLİK İNTRENET BROŞÜR VE AFİŞLER 2021

ESAFETY EYLEM PLANI

eSafety Label - Action Plan

Action plan submitted by Ayşe Çakır for PELİTLİ 75.YIL CUMHURİYET ORTAOKULU - 18.11.2019 @ 11:07:44

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

- 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

- The fact that staff and pupils are allowed to use USB memory sticks in your school following permission, would require that all staff concerned receive adequate training to be able to know when they can be used safely. Is this the case? To keep your systems secure whilst allowing staff and pupils you also need to include the ground rules in your Acceptable Use Policy. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.
- 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/community/using-mobile-device-in-schools).
- Since staff and pupils can use their own equipment on your school network, it is important to make sure that the Acceptable Use Policy is reviewed regularly by all members of the school and adapted as necessary. It must be discussed with pupils at the start of each academic year so that they understand what is in place to protect them and their privacy, and why. Base the policy around behaviour rather than technology. Visitors must also read and sign the Acceptable Use Policy before they use the school's network.

Data protection

- You have a good policy of keeping your learning and administration environments separate. It is good to ensure that staff training on managing these environments is up to date as you continue to review your policies. Share your policy with other eSafety Label users by uploading it to your school profile.
- Your school has a legal obligation under the Data Protection Act (DPA) 1998 to store, archive and dispose of personal information securely. Ensure that a good records management system is put in place. Check the according fact sheet for more information.
- 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.esafetylabel.eu/group/community/safe-passwords.
  Include these rules in your Acceptable User Agreement and avoid giving new users a standard "first access" password.

Software licensing

- It is good practise that the member of staff responsible is fully aware of installed software and their license status.
- 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.
- Compliance with licensing agreements is important. Someone needs to have overall responsibility to ensure that this is happening and that all licenses are valid for purpose. Staff should be briefed on who is the person responsible.
  The End-user license agreement section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

IT Management

Policy

Acceptable Use Policy (AUP)

- Regularly review the Mobile Phone Policy to ensure that it is fit for purpose and that it is being applied consistently across the school. The fact sheets on Using mobile phones at school (www.esafetylabel.eu/group/community/using-mobile-device-in-schools) and School Policy (www.esafetylabel.eu/group/community/school-policy) will provide helpful information.
- 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

- Check that your School Policy includes all necessary information for teachers about handling issues when pupils knowingly or even inadvertently access illegal or offensive material online by going to the guidance set out by the teachtoday.de/en website (tinyurl.com/9j86v84). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form (www.esafetylabel.eu/group/teacher/incident-handling) so that other schools can benefit from your experience.

Staff policy

- 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.
- 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.
- Ensure that all staff, including new members of staff, are aware of the policy concerning online conduct. This should be a topic that is regularly discussed at staff meetings and clearly communicated in the School Policy, and to staff and pupils in the Acceptable Use Policy. Regularly review and update both documents as necessary.

Pupil practice/behaviour

- Your school has a school wide approach of positive and negative consequences for pupil behaviour. This is good practice, please share your policy via the My school area of the eSafety portal so that other schools can learn from it.
- It is good that pupils have the possibility to shape school activities when discussing eSafety, be it extra-curricular and curricular ones, based on what is going on in their daily lives. This way they will be more engaged and it also allows the teacher to recognise real life issues.

School presence online

- 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.
- 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.esafetylabel.eu/group/community/schools-on-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

- 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.
- Technology develops rapidly. Consider sending the member of staff responsible for ICT to trainings and/or conferences regularly to keep them updated on new features and risks. Check out the Better Internet for Kids portal to stay up to date with the latest trends in the online world.

eSafety in the curriculum

- It is good that you are making a specific reference to sexting within your child protection policy as this is a growing issue that many young people are having to deal with. It is also important to ensure that you are providing appropriate education for pupils about this issue.
- 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/community/embedding-online-safety-in-curriculum.
- It is commendable that you are able to provide an eSafety curriculum that keeps up with emerging issues. Continue to make use of new resources as they are made available. Can you upload to your school profile an outline of how you design the curriculum and links to some of the resources you use - this would be most helpful for other schools.
- Sexting is an issue which affects many young people. Sharing possible consequences and risks with them is important, as is the opportunity for some discussion around the issue. Sexting should be part of a broad and balanced eSafety curriculum

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/community/pupils-use-of-online-technology-outside-school

Sources of support

- Dobro je, da staršem nudite podporo v zvezi z e-varnostjo, ko si to želijo. Premislite, ali bi bilo dobro vse starše redno obveščati prek spletne strani ali prek povezav v šolskem e-glasilu. Morda imate lahko tudi roditeljski sestanek. Poglejte si smernice o informacijah za starše na www.esafetylabel.eu/group/community/information-for-parents, kjer boste našli gradiva, ki jih lahko posredujete staršem, in ideje, ki jih lahko uporabite na roditeljskih sestankih.

Staff training

- It is good practise that you provide information to teachers 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. You might want to have a look at the Essle Survey of ICT in schools.
- 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 via the uploading evidence tool, accessible also via the My school area.

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.