

Action plan submitted by Melahat Mattaoğulları for Şehit Sinan Acar Ortaokulu - 16.01.2023 @ 13:02:05

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

- 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.europa.eu/youth/EU\\_en](http://www.europa.eu/youth/EU_en) for examples of discussions that can take place in the classroom on this topic, through role-play and group games.
- It is very good that all your school devices 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.esafetylevel.eu/group/community/protecting-your-devices-against-malware](http://www.esafetylevel.eu/group/community/protecting-your-devices-against-malware).

### Pupil and staff access to technology

- You should organise a meeting with other teachers so you can discuss how the school could use social media and digital devices as an aid to learning in the classroom. Look at the outcomes and report from the SMILE project (Social Media in Learning and Education, <http://www.eun.org/teaching/smile>) to learn more about using social media in the classroom.

### Data protection

- It is good that your email system is protected and that you have a policy for the transfer of pupil data in place. In this regard, it is important to draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines. For further information see the fact sheet on Protecting sensitive data ([www.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools)).
- Having your learning and administration environments together can create a security risk. Ensuring security of staff's and pupils' private data is a fundamental role of the school. We recommend that your appointed eSafety manager/ICT coordinator, together with the staff and a technical expert, define and implement a strategy for separating learning and administration environments or ensuring the equivalent highest level of security between them. Read the fact sheet on Protecting sensitive data in schools at [www.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetylevel.eu/group/community/protecting-sensitive-data-in-schools).

- 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](http://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

- Review the budget for software needs. You might also want to look into alternatives, e.g. Cloud services or open software.
- 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.
- Keeping track of installed software and its licenses is a crucial task in order to avoid expired software licenses and to remain legal within the school ICT infrastructure. Ensure there is an ICT responsible who will be able to produce an overview at any given moment.

## IT Management

- It is good practice to ensure that the person in charge of the ICT network is fully informed of what software is on school-owned hardware and this should be clearly indicated in the School Policy and the Acceptable Use Policy. The person responsible for the network needs to be able to guarantee conformity with licensing requirements and that new software won't interfere with network operation.

# Policy

## Acceptable Use Policy (AUP)

- It is good practise that in your school teachers and pupils sign the relevant school policies and that it is discussed with pupils beforehand. Consider having regular meetings to discuss them and where non-conformity is dealt with.

## 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.
- Keep a central log of any cyberbullying incidents which will help to inform staff about the extent of any potential issues and the type of pupil, age etc. that are affected. Also, be sure that you fill in the eSafety Label [Incident handling form](#). Your input will contribute to building a data base of successful incident-handling practices from schools across Europe that you can use in the future.

- Online issues that take place outside of school will inevitably have an impact inside school. Consider whether the school needs to make a statement about how such issues will be dealt with in the School Policy and the Acceptable Use Policy. Don't forget to anonymously document incidents on the Incident handling form ([www.esafetylabel.eu/group/teacher/incident-handling](http://www.esafetylabel.eu/group/teacher/incident-handling)), as this enables schools to share and learn from each other's strategies.

## 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.esafetylabel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylabel.eu/group/community/using-mobile-device-in-schools)).
- In order to decrease the risks of misuse of user accounts, ensure that you put a procedure in place that immediately informs the ICT responsible to adjust user rights and/or deactivate them if the role of staff or pupil has changed.

## Pupil practice/behaviour

- 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.
- 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.

## School presence 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](http://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.
- Check the fact sheet on Taking and publishing photos and videos at school ([www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school](http://www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school)) 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.

# Practice

## Management of eSafety

- In addition to a clear designation of responsibility to ensure that all necessary network security and user privacy

checks are in place, it is essential that schools also have audit and procedural checks at regular intervals.

Without this, a school will be leaving itself vulnerable. See our fact sheet on School Policy at

[www.esafetylevel.eu/group/community/school-policy](http://www.esafetylevel.eu/group/community/school-policy).

Although there should always be an overall lead person on eSafety just as you have in your school, everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise problems. Use our fact sheet Acceptable Use Policy

([www.esafetylevel.eu/group/community/acceptable-use-policy-aup](http://www.esafetylevel.eu/group/community/acceptable-use-policy-aup)) to ensure that everyone plays their part in ensuring they are all the best and safest digital citizens they can be.

## eSafety in the curriculum

- It is excellent that consequences of online actions are discussed with pupils in all grades. Terms and conditions need to be read to fully understand contractual conditions. This can also concern aspects of data privacy. Another important topic is breach of copyright. Please share the materials used through the uploading evidence tool, accessible also via the [My school area](#).
- eSafety needs to be embedded across the whole 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.esafetylevel.eu/group/community/embedding-online-safety-in-curriculum](http://www.esafetylevel.eu/group/community/embedding-online-safety-in-curriculum).
- It is good that sexting has been integrated into wider online safety education across the school. Are you able to assess the impact of this education? Does it help pupils to modify their behaviours? How do you know?
- It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

## 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.

## 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 great that in your school pupils are actively encouraged to become eSafety mentors. You might want to share your approach to strengthening this network with other teachers on the eSafety Label website via the forum or your school's profile page, so that others can replicate it.
- It is great that you have a staff member which is knowledgeable in eSafety issues who acts as a teacher of confidence to pupils.

## 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/community/cyberbullying](http://www.esafetylabel.eu/group/community/cyberbullying).

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.