

Action plan submitted by Sabriye Güner for Samiye Naim Eğitim Vakfı Ortaokulu - 05.02.2022 @ 15:02:01

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.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).
- It is important that your ICT services are regularly reviewed, updated and removed if no longer in use. Installing the latest versions and patches often addresses security vulnerabilities without which your services might come under attack. Ensure that this is part of the job description of the ICT coordinator.

### Pupil and staff access to technology

- 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.esafetylevel.eu/group/community/using-mobile-device-in-schools](http://www.esafetylevel.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

- › 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).
- › It is good that your school records are stored in a safe environment, it is also necessary that they are archived and disposed with in line with the Data Protection Act. Ensure that a good records management system is put in place. Check the according fact sheet for more information.

## Software licensing

- › Review the budget for software needs. You might also want to look into alternatives, e.g. Cloud services or open software.
- › 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 practise that you are training and/or providing guidance in the use of new software that is installed on school computers. This ensures that school members will take advantage of new features, but also that they are aware of security and data protection issues where relevant.

# Policy

## Acceptable Use Policy (AUP)

- › In your school policy issues are regularly discussed. This is good practice as it ensures staff and pupils are aware of them. Do pupils and staff also have to sign related documents to confirm their awareness?
- › It is good practise that whenever changes are put into place in your school, the school policies are revised if needed. Note though, that also changes outside the school can affect policies such as new legislations or changing technologies. Therefore please review your policies at least annually.

## 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](http://teachtoday.de/en) website ([tinyurl.com/9j86v84](https://tinyurl.com/9j86v84)). If such incidents arise in your school, make sure you anonymously fill out the eSafety Label Incident handling form ([www.esafetymodel.eu/group/teacher/incident-handling](http://www.esafetymodel.eu/group/teacher/incident-handling)) so that other schools can benefit from your experience.

- › 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.
- › 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.esafetymodel.eu/group/teacher/incident-handling](http://www.esafetymodel.eu/group/teacher/incident-handling)), as this enables schools to share and learn from each other's strategies.
- › (Cyber)bullying can be a serious problem and a whole-school approach should be taken to tackle it with a zero tolerance strategy. Read more about it in the eSafety fact sheet area.

## Staff policy

- › 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.
- › 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.esafetymodel.eu/group/community/using-mobile-device-in-schools](http://www.esafetymodel.eu/group/community/using-mobile-device-in-schools)) and ensure that the guidelines to staff are clearly communicated in the School Policy.
- › 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.

## School presence online

# Practice

## Management of eSafety

- › It is good that you have a designated member of staff responsible for eSafety. Consider whether it would be helpful to have an eSafety committee comprising members from all groups of stakeholders. 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](http://www.esafetylabel.eu/group/teacher/incident-handling).

- › 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/community/school-policy](http://www.esafetylabel.eu/group/community/school-policy).

- › 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.esafetylabel.eu/group/community/school-policy](http://www.esafetylabel.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.esafetylabel.eu/group/community/acceptable-use-policy-aup](http://www.esafetylabel.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 good that these issues have been included in the eSafety curriculum. It is a good idea to regularly review the issues which are being covered by your eSafety education in order to ensure that new and emerging issues are covered.
- › 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.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum](http://www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum).

## Extra curricular activities

- › Use Safer Internet Day as a mechanism to get the whole school community involved with online safety. The information and resources available at [www.saferinternetday.org](http://www.saferinternetday.org) offer an ideal opportunity to promote peer advocacy activities.

## 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-](http://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.

- › 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.

## 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.**