

Action plan submitted by HÜSEYİN AYÇİÇEK for 91.000 DEV ÖĞRENCİ ORTAOKULU - 17.01.2023  
@ 12:13:28

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

- › It is good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

### Pupil and staff access to technology

- › 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.
- › 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/community/use-of-removable-devices](http://www.esafetylabel.eu/group/community/use-of-removable-devices) to make sure you cover all security aspects.

### 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.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools](http://www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).
- › 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.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.

- › It is good that your school provides training materials on the importance of protecting devices, especially portable ones. 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.
- › 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

- › 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. The [End-user license agreement section](#) in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.
- › It is good practise that the member of staff responsible is fully aware of installed software and their license status.

## IT Management

- › 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)

- › 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.
- › 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.

## 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](https://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-](http://www.esafetylabel.eu/group/teacher/incident-)

[handling](#)) so that other schools can benefit from your experience.

- › It is a pity not to share the details and solutions applied to bullying incidents both with the staff members and via the eSafety Label incident handling form. Only in this way can you learn through experience and the successful incident handling practices of others. You should also make sure that anti-bullying guidelines are given to pupils and staff in your Acceptable Use Policy.

## Staff policy

- › In your school user accounts are managed in a timely manner. This is important as it decreases the risk of misuse.

## 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.
- › 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.
- › 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

- › 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.esafetymail.eu/group/community/schools-on-social-networks](http://www.esafetymail.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

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

- › 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).

## eSafety in the curriculum

- › It is good practice that all pupils in all year groups in your school are taught about eSafety. It continues to be important to review regularly the curriculum provision to ensure it meets ever-changing needs. If you have a curriculum review process of this kind, it would be helpful to other schools if you could publish this on your school profile. To upload go to your [My school area](#).
- › 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 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.
- › 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?

## Extra curricular activities

- › Gather feedback from pupils to see what sort of additional eSafety support they would benefit from outside curriculum time. Could they be involved in delivering some of this to their peers? Check the resource section on the eSafety Label portal to find resources that will help them do 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](http://www.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school).
- › It is good to know that you are frequently using the online eSafety resources from your national Safer Internet Centre. Have you found these resources helpful in your school? Please send your feedback on their use and value to [info-insafe@eun.org](mailto:info-insafe@eun.org).

## Sources of support

- › It is good to know that other school services are involved in eSafety issues (e.g. counsellors, psychologists, school nurse). Are they also invited to contribute to developing and regular review of your School Policy? Publish a case study about how this is managed in your school on your school profile page on the eSafety Label project website, so that others can learn from your experience.
- › 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

**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.**