

Assessment form submitted by Güler Saraç for Çinikent Özel Eğitim Ortaokulu - 27.12.2022 @ 10:41:58

Infrastructure

Technical security

Question: Are all of your school computers virus-protected?

> **Answer:** Yes, all school computers are virus-protected.

Question: Is the school system protected by a firewall?

> **Answer:** Yes.

Question: Are filtering levels uniform across schools or do they depend on user profiles (teacher, pupil, admin staff, etc.) and their level of maturity/seniority?

> **Answer:** Differentiated levels are applied to different ages of pupils and staff. Staff are able to request that certain sites are unblocked or blocked as appropriate.

Pupil and staff access to technology

Question: Are staff and pupils allowed to use USB sticks on school computers?

> **Answer:** Yes, but how staff and pupils are allowed to use their USBs is clearly stipulated in our Acceptable Use Policy.

Data protection

Question: How is the storage of school records and other documentation dealt with over time?

> **Answer:** We store all school records in a safe environment.

Question: Do you consistently inform all school members about the importance of protecting devices, especially portable ones?

> **Answer:** Yes, we provide training/manuals around issues like these.

Question: How is pupil data protected when it is taken 'off site' or being sent by email?

> **Answer:** All sensitive pupil data is encrypted and stored separately from the learning environment that pupils use.

Software licensing

Question: Do you have an agreed process for installing software on the school system?

> **Answer:** Yes. We have an agreed, effective process.

Question: Does someone have overall responsibility for licensing agreements?

- > **Answer:** Yes.

IT Management

Question: Are teachers and pupils allowed to install software to computers that are school property?

- > **Answer:** No, this can only be done by the person in charge of the school ICT network.

Policy

Acceptable Use Policy (AUP)

Question: Are eSafety issues referred to in other school policies (e.g. behaviour, anti-bullying, child protection)?

- > **Answer:** Some policies refer to eSafety.

Question: How do you ensure the school policies are up to date?

- > **Answer:** Policies are revised adhoc.

Reporting and Incident-Handling

Question: Is there a clear procedure if pupils knowingly access illegal or offensive material at school?

- > **Answer:** Not really, it is up to the individual teacher to deal with this.

Question: Does the school take any responsibility for any online incidents that happen outside the school?

- > **Answer:** Yes, but this responsibility has not been communicated to everyone.

Question: Is there a procedure for dealing with material that could potentially be illegal?

- > **Answer:** It is left to teachers to deal with this when the issue arises.

Staff policy

Question: Is there a School Policy that states how staff should behave online?

- > **Answer:** No.

Question: Do you inform teachers about the risks that come with potentially non-secured devices, such as smartphones?

- > **Answer:** This is the responsibility of the teacher.

Pupil practice/behaviour

Question: Is there a school wide hierarchy of positive and negative consequences to address pupils' online behaviour?

- > **Answer:** Partly - there is a system in place, but this is not consistently applied by all staff or understood by all pupils.

Question: When discussing eSafety related aspects, do pupils have the possibility to shape (extra-curricular and curricular) school activities based on what is going on in their daily lives?

- > **Answer:** Pupils are actively encouraged to choose topics of their interest and/or shape extra-curricular

activities.

School presence online

Question: Is someone responsible for checking the online reputation of the school regularly?

› **Answer:** Not officially, but the ICT coordinator/a senior teacher assumes this role.

Practice

Management of eSafety

Question: How involved are school governors/school board members in addressing eSafety issues?

› **Answer:** There is a named school governor/ board member who reviews eSafety matters.

Question: Technology develops rapidly. What is done to ensure that the member of staff responsible for ICT is aware of new features and risks?

› **Answer:** We leave it up to the member of staff responsible for ICT whether or not to follow up on technology trends and features.

eSafety in the curriculum

Question: Do you talk about online extremism/radicalisation/hate speech as part of your online safety curriculum?

› **Answer:** Yes, we have integrated discussion and education about these issues into our curriculum.

Question: Are legal consequences of online actions discussed with pupils? Topics would include terms and conditions, online payments, copyright.

› **Answer:** Only for the older pupils.

Question: Are pupils taught about the risks of sexting?

› **Answer:** No, sexting is not currently taught at the school.

Özel eğitim öğrencileri olduğu için böyle bir sorunla karşılaşınca bu konu anlatılıyor.

Question: Is the eSafety curriculum progressive?

› **Answer:** Not really; we try to stay as close to the national curriculum as possible.

Extra curricular activities

Question: Does the school have any up-to-date information about the online habits of pupils?

› **Answer:** Yes, we have a little information.

Sources of support

Question: Are there means in place that allow pupils to recognise good practise and expert knowledge in peers with regards to eSafety issues?

› **Answer:** We actively encourage pupils to become peer eSafety mentors by offering facultative courses and/or school rewards on eSafety topics or similar.

Staff training

Question: Are teachers trained on the topic of cyberbullying?

> **Answer:** Yes, every teacher.

Question: Do all staff receive regular training on eSafety issues?

> **Answer:** Some staff occasionally/sometimes receive eSafety training.