eSafety Label - Assessment Form

Assessment form submitted by Handan Halhallı for Şehit Mehmet Çetin İlkokulu - 17.11.2020 @ 08:58:59

Infrastructure

Technical security Pupil and staff access to technology

Question: Are staff and pupils allowed to use their own equipment on the school WiFi network? How is this monitored?

- **Answer:** Staff and pupils are able to access the WiFi using their own personal devices. Use is governed by a robust Acceptable Use Policy, which is agreed and understood by all.

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.

We have virus programs at all school computers. So that we use these programs with security.

Question: Are mobile phones and other digital devices allowed in school?

- **Answer:** Mobile phones are banned on the school site and/or in the classrooms.

Question: What is the pupil/computer access in your school?

- **Answer:** Pupils can bring their own laptops/tablets to school and/or it is easy for the teacher to provide the student with a computer within the class when needed.

Data protection

Question: Do you consistently inform all school members about of 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:** Our email system is protected with passwords and firewalls, and we have rules in place about the transfer of pupil data.

Software licensing

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

- **Answer:** There are a few members of staff that everyone can ask to do this.

Question: Has the school set a realistic budget for the software needs?

- **Answer:** Yes.

It is covered by the school family association budget.

Question: Does someone have overall responsibility for licensing agreements?

- **Answer:** Yes.

IT Management

Question: What happens if a teacher would like to acquire new hard/software for the school network?

- **Answer:** It is up to the head teacher and/or ICT responsible to acquire new hard/software.

Policy

Acceptable Use Policy (AUP)

Question: Does the school have a policy on the use of mobile devices / mobile phones?

- **Answer:** Yes.

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

- **Answer:** They are revised yearly.

Reporting and Incident-Handling

Question: Are incidents of cyberbullying logged centrally?

- **Answer:** No.

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

- **Answer:** Yes. This is included in written guidance for staff.

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

- **Answer:** No.

Staff policy

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

- **Answer:** Yes.

Question: What happens to a teacher's account onces s/he changes her/his role or leaves the school?

- **Answer:** The administrator is informed and immediately deactivates the teacher account or adjusts rights where possible.

Pupil practice/behaviour

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

- **Answer:** Yes and this is clearly understood by all and applied consistently throughout the school.

School presence online

Question: Does your school policy contain a section on the taking and publishing of photographs of, and by, pupils, parents and staff?

- **Answer:** Yes, we have a comprehensive section on this in our School Policy.

Question: Does the school have an online presence on social media sites?

- **Answer:** Yes.

Practice

Management of eSafety

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:** The job description outlines that the member of staff responsible for ICT needs to keep up to date on technologies.

Question: Is there one single person responsible for ICT usage and online access in your school?

- **Answer:** No, teachers are responsible for their pupils' use of ICT and their online safety and security.

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 all pupils in your school taught about eSafety?

- **Answer:** Yes, all pupils in all year groups.

Question: Is eSafety taught as part of the curriculum?

- **Answer:** Yes.

Question: Are pupils taught about their responsibilities and consequences when using social media? Topics would include digital footprints and data privacy.

- **Answer:** Yes, from an early age on.

Extra curricular activities

Question: Does your school celebrate 'Safer Internet Day'?

- **Answer:** Yes, some staff and pupils celebrate 'SID'.

Question: Do pupils do peer mentoring about eSafety?

- **Answer:** Yes, sometimes.

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

- **Answer:** Yes, we have plenty of information.

Sources of support Staff training

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

- **Answer:** Yes, all staff receive regular training on eSafety.

Final comments

> *“We obey all these rules at our education ministiration.We don't need any politicy at our school.“*