

Assessment form submitted by Muhammed Tarakcı for MERAM GÖDENE İLKOKULU - 09.02.2024
@ 13:45:37

Infrastructure

Technical security

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

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

Question: Are existing ICT services regularly reviewed, updated and removed if no longer in use?

- > **Answer:** Yes, this is part of the job description of the ICT coordinator.

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:** There is a basic level of filtering which blocks pornography, violent and illegal content.

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 mobile phones and other digital devices allowed in school?

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

Data protection

Question: Do you have separated learning and administration environments in your school?

- > **Answer:** I don't know.

Question: How are staff and pupil passwords generated for access to your school system?

- > **Answer:** New users are given a standard password and asked to generate their own password on their first access.

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

- > **Answer:** Yes.

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

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

IT Management

Policy

Acceptable Use Policy (AUP)

Question: Does your school have an Acceptable Use Policy (AUP)?

- > **Answer:** Yes, there is an AUP for pupils.

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:** When changes are put into place at school that impact the policy, they are updated immediately.

Reporting and Incident-Handling

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: Are incidents of cyberbullying logged centrally?

- > **Answer:** Yes, we log incidents and also record them via the eSafety Label incident handling form.

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

- > **Answer:** Yes.

Question: Does your school have a strategy in place on how to deal with bullying, on- and offline?

- > **Answer:** Yes, we have a whole-school approach, addressing teachers, pupils and parents. It is also embedded into the curriculum for all ages.

Staff policy

Question: What happens to a teacher's account once 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: Is it possible for pupils to take part in shaping the school online presence?

- > **Answer:** Yes, pupils have the possibility to feedback on our online presence.

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

- > **Answer:** Yes, in all grades.

Question: Do you include sexting and the school's approach to it in your child protection policy?

- > **Answer:** Yes, sexting is referenced in the child protection policy and there are clear guidelines on how to deal with incidents.

Question: Is eSafety taught as part of the curriculum?

- > **Answer:** Yes.

Question: Are pupils taught about the risks of sexting?

- > **Answer:** Yes, sexting is integrated into our eSafety and our sex education teaching at appropriate times.

Question: Are all pupils in your school taught about eSafety?

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

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.

Extra curricular activities

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

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

Sources of support

Question: Does the school provide eSafety support for parents?

- > **Answer:** Yes, when asked.

Staff training

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

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