

Assessment form submitted by Ahmet Kılıç for Menteş Şehit Osman Köse Ortaokulu -
04.01.2023 @ 08:11:15

Infrastructure

Technical security

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.

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.

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

- › **Answer:** There are specific computer labs, which can be booked by the teacher and the teachers make good usage of this option.

Data protection

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.

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 the storage of school records and other documentation dealt with over time?

- › **Answer:** We have a school retention plan specifying how long specific kinds of records are being kept and how they should be archived/disposed of.

Software licensing

Question: Does someone have overall responsibility for licensing agreements?

- › **Answer:** Yes.

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

› **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:** Yes, eSafety is an integral part of several school policies.

Reporting and Incident-Handling

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.

Question: Are incidents of cyberbullying logged centrally?

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

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

› **Answer:** Yes, and all staff, pupils and parents understand this.

Question: Is there a clear procedure detailing what to do if inappropriate or illegal material is discovered?

› **Answer:** Yes.

Staff policy

Question: Are teachers permitted to use personal mobile devices in the classroom?

› **Answer:** In certain circumstances only, in compliance with the AUP.

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

› **Answer:** Yes, we have regularly updated guidelines clearly laid out in the School Policy on this.

Pupil practice/behaviour

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 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.

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: Does the school have a designated member of staff responsible for eSafety?

> **Answer:** It is a shared responsibility for all staff.

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.

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

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: 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.

Question: Is the eSafety curriculum progressive?

> **Answer:** Yes.

Extra curricular activities

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

> **Answer:** Yes, the whole school celebrates 'SID'.

Question: Does the school provide eSafety support for pupils outside curriculum time?

> **Answer:** Yes.

Sources of support Staff training

Question: Are teachers aware about the technology that pupils spend their freetime with?

> **Answer:** Yes, this is part of the training and/or information package provided to teachers.