

Assessment form submitted by Kerim ARI for Hatıp İlkokulu - 29.12.2022 @ 09:15:00

## 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:** No, staff and pupils are not allowed to bring their own personal devices to school.

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

- > **Answer:** Yes, this only requires special permission from the teacher/ICT coordinator.

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

- > **Answer:** Yes, we have separated learning and administration environments.

**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:** 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.

**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.

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

> **Answer:** Once a year we have a staff meeting where decisions about new hard/software are made.

## Policy

### Acceptable Use Policy (AUP)

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

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

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

> **Answer:** Yes.

### 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:** 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.

**Question:** Are incidents of cyberbullying logged centrally?

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

### Staff policy

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

> **Answer:** Yes.

### Pupil practice/behaviour School presence online

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

> **Answer:** Yes.

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

> **Answer:** Yes.

## Practice

### Management of eSafety

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

> **Answer:** Yes.

**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 member of staff responsible for ICT is sent to trainings/conferences at regular intervals.

## 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:** 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.

## Extra curricular activities

**Question:** Do pupils do peer mentoring about eSafety?

> **Answer:** Yes, on a regular basis.

**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:** Can teachers organise a training themselves if they have expert knowledge they would like to share with their colleagues?

> **Answer:** Yes, our school encourages knowledge exchange between staff members. There is also an online community which staff members use.

**Question:** Are teachers trained on the topic of cyberbullying?

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

**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.