Assessment form submitted by Gülüstan Çolak for Şehit Rüstem Resul Perçin Özel Eğitim Okulu - 23.01.2021 @ 21:06:10

Infrastructure

Technical security

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.

> okulumuzda kullanılan internet temel filtreleme vardır

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

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

Pupil and staff access to technology

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: 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 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.

> Okul müdürü saklamakta

Software licensing

Question: Does someone have overall responsibility for licensing agreements?

> **Answer:** No.

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.

> **Okul müdürünüe aittir**

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.

Question: Once new software is installed, are teachers trained in its usage?

> **Answer:** Yes, when we roll-out new software, training and/or guidance is made available.

Policy

Acceptable Use Policy (AUP)

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.

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

> **Answer:** Yes, there is an AUP which covers all members of the school community.

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 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:** Yes.

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 clear procedure if pupils knowingly access illegal or offensive material at school?

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

Staff policy 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 lifes?

> **Answer:** In a limited way.

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: Is someone responsible for checking the online reputation of the school regularly?
> **Answer:** Yes.

Practice

Management of eSafety

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: Does the school have a designated member of staff responsible for eSafety?
> **Answer:** It is a shared responsibility for all staff.

eSafety in the curriculum

Question: Is eSafety taught as part of the curriculum?
> **Answer:** Yes.

Question: Are all pupils in your school taught about eSafety?
> **Answer:** All pupils in some year groups.

> **engelli oldukları için**

Question: Are pupils taught about their responsibilities and consequences when using social media? Topics would include digital footprints and data privacy.
> **Answer:** Yes, but only the older pupils.

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.

Question: Does your school celebrate 'Safer Internet Day'?
> **Answer:** Yes, the whole school celebrates 'SID'.

Sources of support

Question: Do pupils have a means to address a trusted adult in confidence if an online incident occurs outside the school?
> **Answer:** Yes, the school counselor is knowledgeable in eSafety issues.

Question: Does the school provide eSafety support for parents?
> **Answer:** Yes, regularly.

Question: Are there means in place that allow pupils to recognise good practise and expert knowledge in peers

with regards to eSafety issues?

> **Answer:** An informal network of 'eSafety expert' pupils exists.

Staff training