**Background and Rationale**

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school.

The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child’s education from the headteacher to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

* Access to illegal, harmful or inappropriate images or othercontent
* Unauthorised access to / loss of / sharing of personalinformation
* The risk of being subject to grooming by those with whom they make contact on theinternet.
* The sharing / distribution of personal images without an individual’s consent orknowledge
* Inappropriate communication / contact with others, includingstrangers
* Cyber-bullying
* Access to unsuitable video / internet games
* An inability to evaluate the quality, accuracy and relevance of information on theinternet
* Plagiarism and copyrightinfringement
* Illegal downloading of music or videofiles
* The potential for excessive use which mayimpact on the social and emotional development and learning of the youngperson.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, monitoring and review e-Safety Policy

This e-safety policy has been developed and will be reviewed regularly by a e-safety working group made up of:

* SchoolE-SafetyCoordinator Burcu ÜNAL
* Headteacher Yeliz ÜNAL
* SeniorLeader Eyüp YILMAZ
* Support Staff Emek B.ATEŞ
* ICT StrategyManager Döndü T.TOSUN
* ParentRepresentative Sevgi PINAR
* TeacherRepresentative Altan ALTINBAŞ

Schedule for e-Safety Development

|  |  |
| --- | --- |
| This e-safety policy was approved bythe *e-safty school comittee:* | *…...* |
| The implementation of this e-safety policy will be monitored by the: | *E-Safety Coordinator* |
| Monitoring will take place at regular intervals: | *July each year* |
| SchoolE-SafetyCoordinator will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents): | *November each year* |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e- safety or incidents that have taken place. The next anticipated review date will be: | *July each year* |
| Should serious e-safety incidents take place, the following procedure should be followed | *Refer to: Responding to incidents of misuse diagram* |

The school will monitor the impact of the policy using:

* Logs of reported incidents
* Internal monitoring data for network activity by ICT Technicalteam

Scope ofthe Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out ofschool.

Headteachers, to such extent as is reasonable, to regulate the behaviour of students / students when they are off the school site and empowers members of staff toimpose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of theschool.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

**Roles andResponsibilities**

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Headteacher and SeniorLeaders:

* **The Headteacher is responsible for ensuring the safety (including e-safety) of members of theschool community**, though the day to day responsibility for e-safety will be delegated to the E-SafetyCoordinator.
* The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator andother relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, asrelevant
* The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safetynet and also support to those colleagues who take on important monitoring roles. This process will consist of regular reports to the leadershipgroup
* The Senior Leadership Team will receive regular monitoring reports from the E-SafetyCo-ordinator.
* **The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.**
* E-Safety Coordinator:
* leads the e-safetyCo-ordinator
* takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies /documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an e-safetyincident takingplace.
* provides training and advice forstaff
* liaises with the LocalAuthority
* liaises with school ICT technical staff
* receives reports of e-safety incidents which are logged onSIMs
* meets regularly with E-Safety working group to discuss current issues, review incident logs and filtering /change controllogs
* reports regularly to Senior Leadership Team

Technical staff:

ICT Strategy Manager is responsible for ensuring:

* that the school’s ICT infrastructure is secure and is not open to misuse or maliciousattack
* that the school meets the e-safety technical requirements
* that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularlychanged
* theschool’sfilteringpolicyisappliedandupdatedonaregularbasisandthatitsimplementationisnotthesole responsibility of any single person. The e-safety coordinator will coordinate with ICT Technicalteam
* that e-safety coordinator keeps up to date with e-safety technical information in order to effectively carryout their e-safety role and to inform and update others asrelevant
* Subject leaders will liaise with ICT Technical Staff and the e-safety coordinator regarding individual requests for unfiltering based on curriculumneed
* that the use of the network / managed learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action /sanction
* that monitoring software / systems are implemented and updated as agreed in schoolpolicies

Teaching and SupportStaff

are responsible for ensuring that:

* they have an up to date awareness of e-safety matters and of the current school e-safety policy andpractices
* they report any suspected misuse or problem to the E-Safety Co-ordinator /Headteacher / Senior Leader/ Class teacher / action /sanction
* digital communications with students / students should be on a professional leveland only carried out using official schoolsystems
* e-safety issues are embedded in all aspects of the curriculum and other schoolactivities
* students understand and follow the school e-safety and acceptable usepolicy
* students have a good understanding of research skills and the need to avoid plagiarism and upholdcopyright regulations
* they monitor ICT activity in lessons, extra curricular and extended schoolactivities
* they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devicesand that they monitor their use and implement current school policies with regard to thesedevices
* in lessons where internet use is pre-planned students / students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students

* **are responsible for using the school ICT systems in accordance with the Student AcceptableUse Policy, which they will be expected tosign.**
* have a good understanding of research skills and the need to avoid plagiarism and upholdcopyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials andknow how to doso
* will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of imagesand oncyber-bullying.
* should understand the importance of adopting good e-safety practice when using digital technologies outof school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of theschool

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents’ meetings, letters, website and information about national / local e-safety campaigns / literature. Parents will be responsible for:

* endorsing (by signature) the Student Acceptable UsePolicy
* accessing the school website / on-line student records in accordance with the Hilal Necmiye Hüsnü Ataberk Middle School Acceptable UsePolicy

**Policy Statements**

Education –students

Whilst regulation and technical solutions are very important, their use must be balanced by educating to take a responsible approach. The education of *students* in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

* **A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school andoutside school**
* **Key e-safety messages should be reinforced as part of a planned programme of assembliesand tutorial**
* **Students should be taught in all lessons to be critically aware of the materials / content theyaccess online and be guided to validate the accuracy ofinformation**
* **Students should be helped to understand the need for the student policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outsideschool**
* **Students should be taught to acknowledge the source of information used and to respectcopyright when using material accessed on theinternet**
* **Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-onscreens**
* **Staff should act as good role models in their use of ICT, the internet and mobiledevices**

Education – parents / carers

Many parents have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it

The school will therefore seek to provide information and awareness to parents and carers through:

* Letters, newsletters, web site
* Parentsmeetings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried outregularly.
* All new staff should receive e-safety training as part of their induction programme, ensuring that theyfully understand the school e-safety policy and Acceptable UsePolicies
* This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings.
* The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals asrequired

Technical–infrastructure/equipment,filteringand monitoring

**The school ICT Technical team has approved and will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.**

* **ICT network will be managed in ways that ensure that the school meets the e-safety technical requirements outlined by the LocalAuthority**
* **There will be regular reviews and audits of the safety and security of school ICTsystems**
* **Servers, wireless systems and cabling must be securely located and physical accessrestricted**
* **All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technical team and will be reviewed, atleast annually, by the E-Safety Co-ordinator**
* **All users will be provided with a username and password by ICT Technical team who will keep an up to date record of users. Users will be required to change their password every 90days**
* **Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach ofsecurity.**
* **Remote management tools are used by staff to control some workstations and view usersactivity**
* **An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident to the ICT Strategy Manager(or other relevantperson).**
* **Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems anddata.**
* **A procedure is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system. These people should report to the ICT TechnicalTeam**
* **Downloading of executables is done via a Request for Change made to ICT Technicalteam.**
* **Any use of removable media (memory devices, mobile phones etc) must be in line with allschool policies regarding the security of school systems anddata**
* **The school infrastructure and individual workstations are protected by up to date virussoftware.**

Curriculum

**E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.**

* **in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internetsearches.**
* **Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young peoplevisit.**
* **Students should be taught in all lessons to be critically aware of the materials / content theyaccess on-line and be guided to validate the accuracy ofinformation**
* **Students should be taught to acknowledge the source of information used and to respectcopyright when using material accessed on theinternet.**