Abdurrahman iyigün Secondary School e-Safety Policy

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

1.1. Possible statements:

- Abdurrahman İyigün Secondary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

- Abdurrahman İyigün Secondary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

- Abdurrahman İyigün Secondary School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

- Abdurrahman İyigün Secondary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

- The purpose of Abdurrahman İyigün Secondary School online safety policy is to:

  - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Abdurrahman İyigün Secondary School is a safe and secure environment.
  - Safeguard and protect all members of Abdurrahman İyigün Secondary Schoo lcommunity online.
  - Raise awareness with all members of Abdurrahman İyigün Secondary School community regarding the potential risks as well as benefits of technology.
  - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including the, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as ‘staff‘ in this policy) as well as children and parents.

- This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

*1.*2 Writing and reviewing the online safety policy

- Abdurrahman İyigün Secondary Schoo lonline safety policy has been written by the school, involving staff, pupils and parents, with specialist advice and input as required.
- The policy was approved and approved by the school management.
- The school has appointed the Designated Safeguarding Lead Türkan Özgür BEKTAŞ as an appropriate member of the leadership team and the online safety lead.
- The school has appointed assistant director as the member of the Governing Body to take lead responsibility for online safety (e-Safety).
- The online safety (e–Safety) Policy and its implementation will be reviewed by the school/setting at least annually or sooner if required.

1.3 Key responsibilities for the community

1.3.1 The key responsibilities of the school/setting management and leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

* To be aware of any online safety incidents and ensure that external agencies and supportare liaised with as appropriate.

* Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.

* Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.

* Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

* To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
* Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
* To ensure that the Designated Safeguarding Lead (DSL) works with the online safety lead.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

* Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.

* Keeping up-to-date with current research, legislation and trends regarding online safety.

* Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

* Ensuring that online safety is promoted to parents and and the wider community through a variety of channels and approaches.

* Maintaining a record of online safety incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.

* To report to the school management team and other agencies as appropriate, on online safety concerns and local data/figures.

* Liaising with local and national bodies, as appropriate.

* Working with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis with stakeholder input.

* Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

* Contributing to the development of online safety policies.

* Reading the school Acceptable Use Policies (AUPs) and adhering to them.

* Taking responsibility for the security of school/setting systems and data.

* Having an awareness of a range of different online safety issues and how they may relate to the children in their care.

* Modelling good practice when using new and emerging technologies

* Embedding online safety education in curriculum delivery wherever possible.

* Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.

* Knowing when and how to escalate online safety issues, internally and externally.

* Being able to signpost to appropriate support available for online safety issues, internally and externally.

* Maintaining a professional level of conduct in their personal use of technology, both on and off site.

- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

* Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.

* Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.

* To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

* Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.

* Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.

* Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.

* Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

* Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

* Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.

- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 The key responsibilities of children and young people are:

* Contributing to the development of online safety policies.
* Reading the school Acceptable Use Policies (AUPs) and adhering to them.
* Respecting the feelings and rights of others both on and offline.
* Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

* Taking responsibility for keeping themselves and others safe online.
* Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
* Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents:

* Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
* Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
* Role modelling safe and appropriate uses of technology and social media.
* Identifying changes in behaviour that could indicate that their child is at risk of harm online.
* Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

Possible statements:

* The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

* The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

* The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

- Email addresses will be published carefully online, to avoid being harvested for spam .
- Pupils work will be published with their permission or that of their parents.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

Possible statements:

* The school will ensure that all images and videos shared online are used in accordance with the school image use policy.

* The school will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.

* In line with the image policy, written permission from parents will always be obtained before images/videos of pupils are electronically published.

2.3 Official videoconferencing and webcam use for educational purposes

2.3 Possible statements:

* The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

* All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.

- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.

- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

* Pupils will ask permission from a teacher before making or answering a videoconference call or message.
* Videoconferencing will be supervised appropriately for the pupils' age and ability.
* Parents consent will be obtained prior to children taking part in videoconferencing activities.
* Video conferencing will take place via official and approved communication channels following a robust risk assessment.

- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.4 Appropriate and safe classroom use of the internet and any associated devices

2.4 Possible statements:

* Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
* The school/setting's internet access will be designed to enhance and extend education.
* Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
* All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
* Supervision of pupils will be appropriate to their age and ability.
  - Younger pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
  - 8-11 year old pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to

online material and resources which support the learning outcomes planned for the pupils’ age and ability.

  - Teenage pupils will be appropriately supervised when using technology, according to their ability and understanding.

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Use of Personal Devices and Mobile Phones

3.1 Rationale regarding personal devices and mobile phones

3.1 Possible Statements:

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members Abdurrahman İyigün Secondary School community to take steps to ensure that mobile phones and personal devices are used responsibly.

- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use or Mobile Phone Policy

- Abdurrahman İyigün Secondary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents but requires that such technologies need to be used safely and appropriately within schools.

3.2 Expectations for safe use of personal devices and mobile phones

3.2 Possible Statements:

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.

* Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

* The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.

* All members of Abdurrahman İyigün Secondary School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

* All members of Abdurrahman İyigün Secondary School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

- All members of Abdurrahman İyigün Secondary Schoolcommunity will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.

3.3 Pupils use of personal devices and mobile phones

3.3 Possible Statements:

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team.
- If a pupil needs to contact his/her parents they will be allowed to use a school/setting phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the head teacher.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

3.4 Staff use of personal devices and mobile phones

3.4 Possible Statements:

* Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with managers.

* Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

* Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

* Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.

- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- If a member of staff breaches the school/setting policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

3.5 Visitors use of personal devices and mobile phones

3.5 Possible Statements:

* Parents and visitors must use mobile phones and personal devices in accordance with the school acceptable use policy.

* Use of mobile phones or personal devices by visitors and parents to take photos or videos must take place in accordance with the school image use policy.

- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

4. Policy Decisions

4.1. Reducing online risks

4.1 Possible statements:

* Abdurrahman İyigün Secondary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

* Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

* The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.

* The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school/setting computer or device.

* The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

- Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.

4.2. Internet use throughout the wider school/setting community

4.2 Possible statements:

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

4.3 Authorising internet access

4.3 Possible statements:

* The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.

* All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.

* Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

* Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

* When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

5. Engagement Approaches

5.1 Engagement and education of children and young people

5.1 Possible statements:

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

- Education about safe and responsible use will precede internet access.

- Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.

- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.

- All users will be informed that network and Internet use will be monitored.

- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing/ICT programmes of study, covering both safe school and home use.
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

5.2 Engagement and education of children and young people considered to be vulnerable

5.2 Possible statement:

- Abdurrahman İyigün Secondary School is aware that some children may be considered to be more vulnerable online due to a range of factors.

5.3 Engagement and education of staff

5.3 Possible statements:

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.

- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.

* Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.

* All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

5.4 Engagement and education of parents

5.4 Possible statements:

* Abdurrahman İyigün Secondary School recognise that parents have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

* Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in, school prospectus and on the school website.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

6. Responding to Online Incidents and Safeguarding Concerns

Possible statements:

* All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

* All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.

* The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

* Complaints about Internet misuse will be dealt with under the School's complaints procedure.

* Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure

* Any complaint about staff misuse will be referred to the head teacher

* Pupils, parents and staff will be informed of the schools complaints procedure.

* Staff will be informed of the complaints and whistle blowing procedure.

* All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

* All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

* The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

* The school will inform parents of any incidents of concerns as and when required.

* After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

* Parents and children will need to work in partnership with the school to resolve issues.

T.C.
ABDURRAHMAN İYİGÜN ORTAOKULU MD.
MİLLİ EĞİTİM BAKANLIĞI

Haşim DURMUŞ
Müdür