

Şehit Ersoy Yorulmaz Anatolian High School E- Safety Policy

All members of Şehit Ersoy Yorulmaz Anatolian High School have a responsibility to safeguard and promote the welfare of pupils.

This policy promotes safe, healthy, acceptable and effective use of the Internet and other digital tools in school. Furthermore, this policy outlines safe and acceptable working practices for all staff and pupils, ensuring a primary emphasis on safeguarding and welfare of all who use online facilities at Şehit Ersoy Yorulmaz Anatolian High School. Promoting Internet Safety Awareness is as important for staff and parents as it is for pupils, and training, information and special events help to maintain an ongoing focus on acceptable internet use. As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an E-safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

The School Website

The school website is used to provide information, promote the school and celebrate the success of our pupils. The school website safeguards the interests of pupils and staff by: Providing the school address, school email and telephone number as the point of contact. Staff or pupils' home information will not be published;

Photographs that include pupils will be selected carefully, will limited personal information provided; Pupils' full names will not be used anywhere on the school's website, particularly in association with photographs;

The Principal or website manager will take editorial responsibility and ensure that content is accurate and appropriate;

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

No internet user is permitted to:

- * Retrieve, send, copy or display offensive messages or pictures;
- * Use obscene or racist language;
- * Insult or attack others;
- * Damage computer systems or networks;
- * Violate copyright laws;

- * Use another user's password;
- * Use the network for unapproved purposes

The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below. When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet and on social networking sites.

Unsuitable/inappropriate activities School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Şehit Ersoy Yorulmaz Anatolian High School E- Safety Policy

1.1 Aims and policy scope

*Şehit Ersoy Yorulmaz Anatolian High 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.

* Şehit Ersoy Yorulmaz Anatolian High 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.

* Şehit Ersoy Yorulmaz Anatolian High 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.

* Şehit Ersoy Yorulmaz Anatolian High School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

* The purpose of Şehit Ersoy Yorulmaz Anatolian High 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 Şehit Ersoy Yorulmaz Anatolian High School is a safe and secure environment.

*Safeguard and protect all members of Şehit Ersoy Yorulmaz Anatolian High School community online.

* Raise awareness with all members of Şehit Ersoy Yorulmaz Anatolian High School 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 governing body, teachers, support staff, external contractors ,visitors, volunteers and other individuals who work for or provide services on behalf of the school

* 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

The Designated Safeguarding Lead (DSL) are Mrs Zarife Özcan and Mr Özkan Durmaz

The Online safety (e-Safety) lead for the Governing Body is Mrs Sehel Eskiköy Aydoğan

Policy approved by School Headmaster on 1 December, 2020

* Şehit Ersoy Yorulmaz Anatolian High School online safety policy has been written by the school, involving staff, pupils and parents with specialist advice and input as required.

* The policy has been approved and agreed by the Şehit Ersoy Yorulmaz Anatolian High School Governing Body

* The school has appointed the Designated Safeguarding Lead Mrs Zarife Özcan and Mr Özkan Durmaz as an appropriate member of the leadership team and the online safety lead.

* 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 Şehit Ersoy Yorulmaz Anatolian High School 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 support are 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 (or committee, board member as appropriate) is identified with a lead responsibility for supporting online safety.

1.3.2 The key responsibilities of the Şehit Ersoy Yorulmaz Anatolian High School 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 carers and the wider community through a variety of channels and approaches.
- * Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- * Maintaining a record of online safety concerns/incidents and actions taken as part of the schools

safeguarding recording structures and mechanisms. (It is recommended that schools and settings record online safety within existing child protection/safeguarding procedures and files to achieve this)

- * Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- * To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- * Ensuring that online safety is integrated with other appropriate school policies and procedures.
- * Leading an online safety team/group with input from all stakeholder groups.
- * Meet regularly with the governor/board/committee member with a lead responsibility for online safety.

1.3.3 The key responsibilities for Şehit Ersoy Yorulmaz Anatolian High School 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.

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/setting'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.

1.3.5 The key responsibilities of Şehit Ersoy Yorulmaz Anatolian High School students are:

- * Contributing to the development of online safety policies.
- * Reading the school/setting 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 and carers are:

- * Reading the school/setting 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 Şehit Ersoy Yorulmaz Anatolian High School website

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

* The head teacher Mrs Sehel Eskiköy Aydoğan 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 (e.g. by replacing '@' with 'AT'.)

* Pupils work will be published with their permission or that of their parents/carers.

* 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

* Şehit Ersoy Yorulmaz Anatolian High School will ensure that all images and videos shared online are used in accordance with the school image use policy.

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

2.3 Managing email

*** All members of staff are provided with a specific school/setting email address to use for any official communication.**

* The use of personal email addresses by staff for any official setting is not permitted.

* The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

* Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure email.

* Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.

* Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.

Whole -class or group email addresses may be used for communication outside of the school (in early years, infant and primary schools).

*Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

*Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

*The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

* School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use for educational purposes

* 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 and carers 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.

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

* 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.

* The school'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.

* 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 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. Social Media Policy

3.1. General Social Media Use

* Expectations regarding safe and responsible use of social media will apply to all members of Şehit Ersoy Yorulmaz Anatolian High School community and exist in order to safeguard both the school and the wider community, on and offline.

* All members of Şehit Ersoy Yorulmaz Anatolian High School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

* Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Şehit Ersoy Yorulmaz Anatolian High School community.

* All members of Şehit Ersoy Yorulmaz Anatolian High School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

* Şehit Ersoy Yorulmaz Anatolian High School will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems

* Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.

* Any concerns regarding the online conduct of any member of Şehit Ersoy Yorulmaz Anatolian High School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

* Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Official use of social media

***Şehit Ersoy Yorulmaz Anatolian High School official social media channels are:**

* Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.

* All communication on official social media platforms will be clear, transparent and open to scrutiny.

* Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

- * Official social media use will be in line with existing policies including anti-bullying and child protection.
- * Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- * Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- * Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.
- * Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- * Parents will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- * Public communications on behalf of Şehit Ersoy Yorulmaz Anatolian High School will, where possible, be read and agreed by at least one other colleague.
- * Official social media channels will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.
- * Şehit Ersoy Yorulmaz Anatolian High School will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff personal use of social media

- * The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- * Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- * All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles Designated Safeguarding Lead and/or the headteacher.
- * If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- * All communication between staff and members of the school community on school business will take place via official approved communication channels (such as an official setting provided email address or phone numbers)
- * Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

* Any communication from students/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

* Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

* All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

* All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

3.4 Staff official use of social media

* If members of staff are participating in online activity as part of their capacity as an employee of the school then they are requested to be professional at all times and to be aware that they are an ambassador for the school.

* Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.

* Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.

* Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.

* Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

* Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

* Staff will not engage with any direct or private messaging with children or parents through social media and will communicate via official communication channels.

* Staff using social media officially will sign the school social media Acceptable Use Policy.

3.5 Pupils use of social media

* Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.

* Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

* Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

* Pupils will be advised not to meet any online friends without a parent or other responsible adult's permission and only when they can be present.

* Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

* Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

* Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

* Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

* Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

* The widespread ownership of mobile phones and a range of other personal devices among young people and adults will require all members Şehit Ersoy Yorulmaz Anatolian High 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

* Şehit Ersoy Yorulmaz Anatolian High 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

4.2 Expectations for safe use of personal devices and mobile phones

* 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. Şehit Ersoy Yorulmaz Anatolian High School accepts no responsibility for the loss, theft or damage of such items.

* Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms

* 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.

* Members of staff will be issued with a work phone number and email address where contact with pupils or parents is required.

* All members of Şehit Ersoy Yorulmaz Anatolian High School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

4.3 Pupils use of personal devices and mobile phones

* 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.

* Pupil's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons.

*Mobile phones or personal devices will not be used by pupils during lessons or formal school time

* If a student needs to contact his/her parents they will be allowed to use a school 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 headteacher.

*Students should protect their phone numbers by only giving them to trusted friends and family members.

* 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.

4.4 Staff use of personal devices and mobile phones

* 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 leaders/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 policy then disciplinary action will be taken.

4.5 Visitors use of personal devices and mobile phones

- * 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.

5. Policy Decisions

5.1 Online risks

- * 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 students 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 computer or device.

5.2. Internet use throughout the wider school community

- *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 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

5.3 Authorising internet access

- * 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 the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- * 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 school's internal online safety (e-Safety) education approaches.
- * The school will reward positive use of technology by pupils.

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

Şehit Ersoy Yorulmaz Anatolian High School is aware that some children may be considered to be more vulnerable online due to a range of factors.

6.3 Engagement and education of staff Relevant for all settings

* 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.

* 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.

6.4 Engagement and education of parents and carers

* Şehit Ersoy Yorulmaz Anatolian High 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 newsletters, letters, school prospectus and on the school website.

E safety for parents

E-Safety is an important part of keeping pupils safe at Şehit Ersoy Yorulmaz Anatolian High School. We have extensive security measures in place in school, monitored both internally and externally, to help safeguard pupils from potential dangers or unsuitable material. Any E-Safety incidents are managed in accordance with our Online Safety Policy. Computing sessions, examining how to stay safe and behave appropriately online.

We can only be successful in keeping children safe online if we work with parents to ensure the E-Safety message is consistent. It is important that parents discuss with their children about how they can keep themselves and their data safe and behave appropriately online.

Social Media use can be one of the biggest concerns for parents regarding their child's use of the internet.

It is important to be realistic – banning a child from using the Internet or other technologies is not the answer, we need to educate our children in their responsible and safe use and ensure that they know who they can speak to if they feel threatened or unsure by anything they come across.

Appropriate use of the internet continues at home, where school work and study can benefit from the wealth of resources available. The school advises parents to provide filtered and supervised use of the internet at home, and the following guidance is provided:

Discuss with your child the rules for using the internet and decide together when it should be used, for how long and for what purposes;

Get to know the sites your child is visiting, and talk with them about what they are learning;

Ensure that you give agreement before your child gives out any personal information on the internet, such as a picture, an address, a phone number, the school name or financial details;

Encourage your child to avoid responding to any unwelcome, unpleasant or abusive messages, and to tell you if they receive any such messages and the school must be informed immediately.

GAMES

Games have changed radically in the last 20 years, which can present an issue to many parents who may not understand or appreciate the content contained within them. 25 years ago, video games were designed for one audience – children. But things have moved on quite radically since then. Games like Super Mario, Sonic and even arcade games like Pac-man were fun, simple and child-friendly. Then in the mid 1990's this changed when a game called Mortal Kombat was released – a game which, although not the first inappropriate game, was certainly the first to kick off a debate which still rumbles on today. Now, games such as Grand Theft Auto (GTA), Call of Duty (COD) and Saint's Row (to name a few) are getting released at regular intervals; games are no longer just about running around collecting gold coins or rings. Games these days deal with incredibly complex social and political issues such as war, terrorism, human trafficking, rape, prostitution, drug and alcohol abuse, and can also be seen to promote incredibly sexist views towards women - many characters refer to women using derogatory terms, which we won't go into here, and see them as objects. Role models in video games are no longer hero's like Mario or Link (the hero in Zelda), but individuals who glamorise law breaking, are morally ambiguous and settle their differences through violence and terror, using language which would make even the hardiest of parents shudder at the thought of their children hearing. If you're unsure if a game is appropriate or not, all you need to do is walk in the shop, grab the game and check out the guidance. If it says 18, it's for adults! Just view the rating the same as you would for a film. It's also worth remembering that if they are playing an 18 rated game online, they will be playing with other adults who will talk about things in a way which is not appropriate for your child to hear. If you're still not sure whether or not the game is appropriate, even with the rating to help, try looking on YouTube for videos showing the game being played. This can be a great way to familiarise yourself with the virtual world they want to play in before they get a chance to experience it. Excessive gaming, especially late night gaming, can affect concentration levels during the school day as children can be overly tired and irritable. It can also make it more difficult for them to settle at night, keeping their brain active when they are trying to get to sleep. It's also important to encourage frequent breaks for them so they do not remain sat in the same position. for too long. Many games are set in the 'real world' with many characters in games committing acts of crime or violence with a blatant disregard for human life and laws of the land which they may come to see as normal behaviour in real life. It can also promote very negative views of women, including violence towards women being seen as 'normal'. With the best will in the world, even if you say no, your children may borrow games from their friends to play at home or play round their friend's house. Games consoles are also more likely to end up in bedrooms than living rooms which will keep their virtual world hidden from you. To keep you in control of the games they are playing, try these top tips:

-It isn't really practical these days, but if possible (particularly for younger players) keep the console in a family friendly room. This allows you to keep an eye on who they are playing

with, the content within the game as well as helping you to learn more about the games they play or enjoy playing

- Remember that games consoles allow you to play online with strangers, ask them who they play games with and how they know them – make sure they aren't giving away too much information about themselves while playing with 'friends'

- Ensure that before your child plays any games online, they know how to 'block' individuals who may cause them problems. This is their front line of defence against anyone who may wish to spoil their fun. Get them to show you how to do it before you let them loose!

- Make sure they understand when to report someone and also understand that they could be reported if they break the rules.

- Encourage them to take breaks every hour or so (parental controls can force this to happen, even showing a timer so they know how long they have left).

Playing games with your friends can be such a positive and enjoyable experience, some games can be educational (Minecraft), teaching appropriate moral values and inspiring the creative genius within, others are simply brilliant, silly fun. Providing we ensure the games are appropriate, we should let children enjoy experiencing these hugely appealing virtual playgrounds while still ensuring that we, the parents, can keep an ever watchful eye on what kind of worlds they are visiting.

Pupil Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Agreement.

If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines

Name of Pupil:.....

Class:

Signed:

Date:

I will only log-on with my own user name and password

I will follow the school's ICT security system and not reveal my password to anyone. I will change my password regularly

I will make sure that all ICT communication with pupils, teachers or others is responsible and sensible
I will be responsible for my behaviour when using the internet. This includes resources I access and language I use

I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher

I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher

Images of pupils and/or staff will only be taken, sorted and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the principal.

I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute

I will respect the privacy and ownership of others' work online at all times,

I will not attempt to bypass the internet filtering system

I understand that all my use of the internet and other related technology can be monitored and logged and can be made available to my teachers

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/guardian will be contacted

