GÜZELYURT KIZ ANADOLU İMAM HATİP LİSESİ

E-SAFETY POLICY

Issued Date: November 2022

Our Vision
The most important vision of the school is to increase the quality of education and to achieve success in education in cooperation between students and parents.

Approved By: Headmaster

Güzelyurt Kız Anadolu İmam Hatip Lisesi

https://guzelyurtaihl.meb.k12.tr

02128543525

34510 ESENYURT/İSTANBUL

CONTENTS PAGE

1. INTRODUCTION AND OVERVIEW

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Güzelyurt Kız Anadolu İmam Hatip High School with respect to the use of ICT-based technologies.
- Safeguard and protect the pupils and staff of Güzelyurt Kız Anadolu İmam Hatip High School
- Assist school staff working with pupils to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimize the risk of malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarized as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites, including radicalization and extremism.

Contact

- Grooming.
- Cyber-bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook,Twitter,Instagram,EBA profiles)) and sharing passwords.
- Radicalize.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online (internet or gaming)).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership - such as music and film).
- Being drawn into terrorism or supporting terrorism.

Scope

This policy applies to all members of Güzelyurt Kız Anadolu İmam Hatip High School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school ICT systems.

The Education and Inspections Act 2010 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

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

Role	Key Responsibilities
Headmaster	• To take overall responsibility for e-safety provision. • To take overall responsibility for data and data security (SIRO). • To ensure the school uses a robust, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the E-Safety Coordinator / Officer. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. Network manager).
E-Safety Coordinator / Designated Safeguarding Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-safety education is embedded across the curriculum. • Liaises with school ICT technical staff. • To communicate regularly with the designated e-safety governor / committee to discuss current issues, review incident logs and filtering / change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

Role	Key Responsibilities
	• To ensure that an e-safety incident log is kept up to date. • Facilitates training and advice for all staff. • Liaises with the local authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • Sharing of personal data • Access to illegal / inappropriate materials • Inappropriate on-line contact with adults / strangers • Potential or actual incidents of grooming • Cyber-bullying and use of social media • Accessing potential extremist sites • Liaise with and educate parents and raising awareness as instructed by head
Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe. • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. • To support the school in encouraging parents to become engaged in esafety activities. • The role of the E-Safety Governor will include regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs).
ICT Teacher / Lead	• To oversee the delivery of the e-safety element of the Computing curriculum. • To liaise with the e-safety coordinator regularly.
Network Manager	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy. • To ensure that provision exists for misuse detection and malicious attack e.g. Keeping virus protection up to date). • To ensure the security of the school ICT system. • To ensure that access controls exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web filtering is applied and updated on a regular basis. • That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Deputy Head	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.

Role	Key Responsibilities
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the e-safety coordinator. • To maintain an awareness of current e-safety issues and guidance e.g. Through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. Email, text, mobile phones etc.
Pupil	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's ESafety Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children. • To consult with the school if they have any concerns about their children's use of technology.
Role	**Key Responsibilities**
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and copy kept in the Staff Room.
- Policy to be part of school induction pack for new staff.
- Acceptable Use agreements discussed with pupils at the start of each year.
- Acceptable Use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

Handling complaints

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - Interview/counselling by Year Tutor /E-Safety Coordinator / Headteacher.
    - Informing parents or carers.
    - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination controlled Assessments].

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and monitoring

The e-safety policy is referenced from within other school policies: Staff (AUP) Acceptable Use Policy, Pupil (AUP) Acceptable Use Policy, Safeguarding Policy, Anti-Bullying policy and in the Behaviour Policy.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been drawn up by e-safety team members and is current and appropriate for its intended audience and purpose.
- The e-safety policy has been agreed by the SLT and approved by Governors. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff.

2. EDUCATION AND CURRICULUM

Pupil e-safety curriculum

Güzelyurt Kız Anadolu İmam Hatip High School:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and

experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. Be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files - such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. Parent or carer, teacher or trusted staff member, or an organization such as child line or CEOP (Child Exploitation & Online Protection).

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through the Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behavior in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; online gaming / gambling.

Staff and governor training

Güzelyurt Kız Anadolu İma Hatip High School:

- Makes staff aware of safety as and when necessary through email updates/ termly staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safety policy and the school's Acceptable Use Policies.

Parent awareness and training

Güzelyurt Kız Anadolu İmam Hatip High School:

- Will initiate and run a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safety behavior are made clear.
    - Information leaflets; in school newsletters; on the school web site.
    - Suggestions for safe Internet use at home.

3. EXPECTED CONDUCT AND INCIDENT MANAGEMENT

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- 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 images and on cyber-bullying Staff.
- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
- Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident management

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behavior of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- Support is actively sought from other agencies as needed (e.g. The local authority, Turkey safer internet centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and reported to the school's senior leaders, governors.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law ie.. visiting extremist sites.

4. MANAGING THE ICT INFRASTRUCTURE

Internet access, security (virus protection) and filtering

Güzelyurt Kız Anadolu İmam Hatip High School:

- Has the filtered secure broadband connectivity through Ministry of National Education of Turkish Republic recognized Provider which provides basic in built filtering in all Turkish schools.
- Uses MEB (Ministry of National Education) filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Ensures network health through use of Norton, Avast, Kaspersky anti-virus software etc. and network set-up so staff and pupils cannot download executable files.
- MEB (Ministry of National Education) internet system blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only unblocks sites for specific purposes / Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites - except those approved for educational purposes.
- Uses security time-outs on Internet access where practicable / useful.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns.

- Ensures pupils only publish within an appropriately secure environment as and when it is part of the curriculum as directed by Teachers.
- Informs all users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the Teacher or Deputy Head (or another staff member who will escalate accordingly).
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse - through staff meetings and school assemblies.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities such as the Police.

Network management (user access, backup)

Güzelyurt Kız Anadolu İmam Hatip Lisesi High School:

- Uses individual, audited log-ins for users.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful.
- Ensures the Systems Administrator / network manager is up-to-date with relevant policies.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Güzelyurt Kız Anadolu İmam Hatip High School:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. We provide a different username and password for access to our school's network to their e-mail system.
- We provide pupils with an individual network log-in username from Year 13 for which they are also expected to use a personal password.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off/shut down when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then logon again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
- Will be setting the network so that users cannot download executable files / programmes.
- Has blocked access to music/media download or shopping sites - except those approved for educational purposes.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by H&S Officer. Equipment installed and checked by approved electrician.

- Does not allow any outside Agencies to access our network.
- Makes clear responsibilities for the daily back up of all systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure back up of critical data.
- Uses a dedicated network for our CCTV system and have had set-up by approved installers.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils (where they have been given an individual account) must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique and strong username and private passwords to access all school systems. Staff are responsible for keeping their passwords private.

E-mail

This school:

- Provides staff with an email account for their professional use, School Office 365 email and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of Microsoft provided technologies to help protect users and systems in the school, including desktop anti-virus product (Avast,Norton,Kaspersky) plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. In support of these filtering (e.g. Open DNS/Talk Talk Work Safe) monitors and protects our Internet access to the World Wide Web.**Pupils:**

Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

- Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
- That an e-mail is a form of publishing where the message should be clear, short and concise.
- They must not reveal private details of themselves or others in e mail

telephone number, etc.

- To ‘stop and think before they click’ and not open attachments unless sure the source is safe.
- That they should think carefully before sending any attachments.
- That they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying/extremist in nature.
- Not to respond to malicious or threatening messages.
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
- That forwarding ‘chain’ e-mail letters are not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff should only use the School Office365 e-mail systems on the school system.
- Staff only use School Office365 e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.

- Staff know that e-mail sent to an external organization must be written carefully, (and may require authorization), in the same way as a letter written on school headed paper.
  - The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
  - The sending of chain letters is not permitted.
  - Embedding adverts is not allowed.
- All staff sign our school Agreement Form AUP to say they have read and understood the esafety rules, including e-mail and we explain how any inappropriate use will be dealt with.School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorizers: e.g. Website administration officer.
- Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs published on the web do not have full names attached.
- We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school /academy or local authority.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation.

5. DATA SECURITY: MANAGEMENT INFORMATION SYSTEM ACCESS AND DATA TRANSFER

Strategic and operational practices

At this school:

- The Headmaster is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one single central record in the admin office.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - Staff.
    - Pupils.
    - Parents.
- This makes clear staffs' responsibilities with regard to data security, passwords and access.
    - We require that any restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
    - We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lockout after a determined amount of idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We store any sensitive written material in lockable storage cabinets in a lockable storage area.

- All servers are in lockable locations and managed by DBS-checked staff.
- Backups are stored in lockable locations.
- We use a secure back-up solution for disaster recovery on our network server(s).
- Paper based sensitive information is shredded, using cross cut shredder.
- We use DBAN secure file/hard disk deletion software as and when required.

6. EQUIPMENT AND DIGITAL CONTENT

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be handed into the school office before registration. They can be picked up at the end of the school day. Staff members may only use their phones out of teaching time.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorized use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorization for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones only out of teaching time. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- The School strongly advises that students bringing mobile phones and mobile devices into school should hand them into the school office before registration.
- If a student breaches the school policy by not handing her mobile phone or mobile device into the school office, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- The school accepts no responsibility for the loss, theft or damage of personally-owned mobile

phones or mobile devices that pupils do not hand into the school office.

- During study leave, phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, 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.
- Students should protect their phone numbers by only giving them to trusted friends and family members.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school - name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.

- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- All redundant equipment will be disposed of through authorized means only with Head Teacher approval.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations. Further information can be found on the Environment Agency website.

7. VERSION HISTORY

Issue Date	Version Number	Approved By
November 2022	1.0	Headmaster