ACORNS INTERNATIONAL SCHOOL

INSPIRING AND EMPOWERING

E-SAFETY POLICY

Reviewed: April 2022

ICT in the 21st Century is seen as an essential resource to support learning and teaching. It plays an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies to equip young people with the skills to access life-long learning and employment.

Reviewed by:

Shirin Bagchi
Head of Secondary Department

This policy must be read and understood in concurrence with AIS Academic Integrity Policy, Device Usage Policy, Behaviour and Discipline Policy.

E-Safety Policy

We believe this policy should be a working document that is fit for purpose, represents the school ethos, and enables consistency.

Introduction

In the 21st Century, Information and Communications Technology (ICT) is increasingly an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these emerging technologies to equip learners with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the technological advancement and fast paced evolution of ICT within our society as a whole. Currently students use the internet both inside and outside of the classroom for several purposes, such as:

- Website browsing and development
- Platform Forums and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Conferences and Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smartphones with text, WhatsApp, google Chats, Video and/ or Web Functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not regulated consistently. All users need to increase awareness about risks associated with the use of these Internet technologies.

At Acorns International School (AIS), we understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate usage and critical thinking skills to ensure safe and legal implications of using the internet and related technologies, in and out of the classroom.

Schools have databases containig information of personal data on learners, staff and other people conducting day-to-day activities. Some of this information is confidential and requires to be kept safely. The inadequate storage of confidential information and leakage to the media and publishing house, may potentially result in publication and damage the reputation

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them (see Data protection policy and GDPR guidelines for more information).

This policy for (for all staff, directors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, mp3 players and portable media players, etc).

Internet Use in School

- In school, students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- We use MikroTik Firewall to filter out unwanted or inappropriate websites.
- All users need to be aware that Internet use is monitored internally by the school's network manager. This includes e-mail communication.
- Staff will preview any recommended sites before using
- Raw image searches are discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that students are given a written list of recommended sites.
- It is advised that parents recheck these sites and supervise this work. All users must observe copyright of materials from electronic resources and follow academic integrity by using proper citations and acknowledgements for the work submitted, failure to do so may lead to consequences as laid down in AIS Academic Integrity Policy.
- No personal information should be given out which could compromise the safety and interests of the user.
- Care and restraint needs to be exercised regarding the publishing of opinions and comments online. These are subject to the same laws of libel and defamation as wider media (newspapers and broadcast media). At AIS, we maintain a 'zero tolerance' policy towards bullying, both online and offline. Hence such actions may lead ot harsh consequences and even expulsion. Please read our Behaviour and Discipline Policy for further reference.
- It is worth reiterating here the main rules: no online gambling, no downloading of software or .exe files. No interfering with security settings and anti-virus software. Passwords, usernames and personal account details must never be shared or made public. The students are not allowed to use their own internet services while on campus. If any student is found using personal internet providers, there will be consequences, even leading to expulsion.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the HoDs.
- Staff and students must consider the appropriateness of any images they post due to the difficulty of removing an image once online. They must also be aware that Images, once online, can be replicated, manipulated and changed.

Managing E-Mail

- The school gives all e-mail account to use for academic work. This email enables to minimise the risk of receiving unsolicited or malicious e-mails and avoid the risk of personal profile information being revealed
- It is the responsibility of each account holder and the school's network manager, to keep the password secure. For the safety and security of users and recipients, all mail

is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all academic work

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to parents or pupils must cc. the head / deputy of department, or line manager
- Students may only use school approved accounts (these will be given to pupils) on the school system during the school day and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information. You must therefore actively manage your e-mail account as follows:

    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives. Information received through emails should follow the same guidelines for erasure as digital or paper documents.

- The forwarding of chain letters is not permitted in school.
- All students e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission. This goes for the Email chat service and WhatsApp and other messaging service providers.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive or suspect e-mail
- Staff must inform(Head/ Deputy of department) if they receive an offensive or suspect e-mail
- Students are introduced to e-mail as part of the ICT Scheme of Work
- However, when you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply
- Never open attachments from an untrusted source; Consult your network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

E-Safety in the Curriculum

- Students- E-Safety in the curriculum ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.
- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The E-Safety policy will be introduced to the students at the start of each school year
- The school has a framework for teaching Internet skills in ICT
- The school provides opportunities within a range of curriculum areas to teach about E-Safety

- Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies;

  i.e. parent/ carer, teacher/ trusted staff member

  Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum**.**

Staff – E-Safety

- New staff receive information on the school's acceptable use policy as part of their induction
- Staff receive annual training and updates on safety as part of their CPD training.

Incident Reporting

Any serious security breaches and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Network manager. This includes lost/stolen equipment/data, virus notifications, and unsolicited emails. Any data breaches must also be reported to the Data Protection Officer.

All Internet activity is logged by the school's internet provider. These logs may be monitored by authorized Staff.

A breach or suspected breach of policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

E-Safety Incident Log

Some incidents may need to be recorded separately if they relate to a bullying or racist incident.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
-
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Workstations should be locked when not in use.
- Be aware if students viewing passwords being entered and keep doors locked when not in the room.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords (complex) each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal complex password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff deactivate on the date of leaving employment and students who have left the School. Information is stored for ***one month.***

If you think your password may have been compromised or someone else has become aware of your password, report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff and pupils are expected to have secure complex passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share them with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy and Data Security
- Users are provided with an individual network and email
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our school, all ICT password policies are the responsibility of **the Network Manager** and all staff and students are expected to comply with the policies at all times

Remote Access (e.g. accessing e-mail and e-portal from home)

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Safe use of Images

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you on what actions to take and be responsible for advising others that need to know

Using Images and Film

See the Photography policy for information on the use of digital images and film.

Electronic Equipment Brought into School

Acorns International School has a Bring Your Own Device initiative. Students in Year 10 and higher will be able to bring laptops, netbooks or tablets to use for educational purposes. Students in lower years will not be allowed to bring any technological devices to school in alignment with previous AIS policies

This relates to portable computers, tablets, memory sticks, external hard-drives, and mobile devices.

These are subject to the same conditions stated in the Device Usage Policy. Inappropriate content and unacceptable use will be viewed by the school as serious infringements and appropriate action will be taken.

Responsibility for these devices is with the owner.

Whilst every effort will be made to deter and punish theft, damage or vandalism, Acorns International School will not necessarily investigate every case of damage or theft.

As part of GDPR guidelines, all removable storage systems should be password protected. Devices should be ones used for school purposes only and should not mix with external/personal data and information.

School data should not be stored on personal computers.

Parental Involvement

We believe that it is essential for parents/ guardians to be fully involved with promoting E-Safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/ guardians and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ guardians and students are actively encouraged to contribute to adjustments or reviews of the school E-Safety policy via the CEO***)***
- Parents/ guardians are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ guardians are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to E-Safety where appropriate in the form of;
    - Information Evenings
    - Website/Learning-Platform Postings
    - Newsletter Items
    - Official WhatsApp Groups
    - Email and ManageBac Announcements

The Data Protection Officer

The DPO is a senior member of staff who is familiar with information risks and the school's response. The DPO has the following responsibilities:

- They own the information risk policy and risk assessment
- What information is held, and for what purposes
- What information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of See Data protection Policy for more information.

Review Procedure

There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them

There will be an on-going opportunity for staff to discuss with the DPO any issue of data security that concerns them

This policy will be reviewed every 36 months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted

INTERNET SAFETY

S — Stay Safe

- Keep your personal information and passwords private
- Never use your real name as your username
- Do not give out your personal information to people or companies you do not know

M — Don't Meet Up

- Never meet with an online friend, even if you think you know them well
- Online friends are still strangers and may not be who they say they are

A — Accepting Files

- Do not open e-mails from people you do not know
- Emails and attachments can contain viruses or unpleasant images

R — Reliable?

- Not all information online is reliable, always check that information is correct before using it
- False identities are used a lot in chat rooms, try to limit to real friends

T — Tell Someone

- Tell an adult if anything online makes you feel uncomfortable
- Log off if you feel uncomfortable or suspicious of anything
- Most chat rooms and social media have alert buttons to report bullying or inappropriate behaviour

CLICK CEOP
Internet Safety

Smile and Stay Safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Social Media

The Widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to data protection and safeguarding children young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff in the school.

The purpose of the policy is to:

- Protect the school from legal risks
- Ensure that the reputation of the school, its staff and directors is protected
- Safeguard all children
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school

Definitions and Scope:

Social networking applications include, but are not limited to: blogs, online discussion forums, collaborative spaces, media sharing services, microblogging applications, and online gaming, environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Last.fm, and comment streams on public websites such as newspaper site.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds. All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection (GDPR) and freedom of information legislation. They must operate in line with the school's Equalities, Child protection and ICT acceptable use policies.

School personnel should use social networking sites wisely and cautiously and if absolutely necessary bearing in mind they should not jeopardize themselves, others or their place of work. The school will monitor its IT system for inappropriate usage and will take the necessary disciplinary measures if need be.

Within this policy, there is a distinction between the use of school sanctioned social media for professional educational purposes, and personal use of social media.

Use of Social Media in practice:

- Personal use of social media
  - Use only your name for the profile.
  - Do not put your date of birth on the profile.
  - Make your profiles 'invite' only and thus only allow people you trust with certainty to view your information.
  - School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at Acorns International School.
  - Any communication from children on any personal media sites must be reported to the designated person for Child Protection (HoD or LSS Department).
  - If any member of staff is aware of any inappropriate communications involving any child on any social media, these must immediately be reported as above.
  - School staff are strongly advised to set all privacy settings to the highest possible level on all personal social media accounts.
  - All email communication between staff and the school community on school business must be made from an official school email account.
  - Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the CEO.
  - Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
  - Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts.
  - Staff should not accept any current student of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account
  - We strongly recommend that school personnel do not use the school's IT system to access social networking sites for their own personal use.

School sanctioned and the use of social media:

There are many legitimate uses of social media within the curriculum and to support student learning. There are also many possibilities for using social media to enhance and develop students' learning.

When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.
- The URL and identity of the site should be notified to the appropriate Head of Faculty or member of the SMT before access is permitted for students.
- The content of any-school-sanctioned social media site should be solely professional, and should reflect well on the school. Do not place derogatory, defamatory, discriminatory or offensive remarks about the school, work colleagues, parents, students, directors or anyone else connected with the school.
- Be careful what viewpoints you express (political, religious).
- Staff must not publish photographs of children without the consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.
- Care must be taken that any links to external sites from the account are appropriate and safe.
- Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to a member of SMT
- Staff should not engage with any direct messaging of students through social media where the message is not public
- All social media accounts created for educational purposes should include a link in the ' About' or 'Info' page to the ICT Acceptable Use Policy on the school website. This will indicate that the account is officially sanctioned by Acorns International School
- We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

ACORNS INTERNATIONAL SCHOOL
INSPIRING AND EMPOWERING

Student Acceptable Use - Agreement / E-Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behavior when using the Internet. This includes resources I access and the 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 students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Head / Deputy of MYP.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line 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 technologies 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 may be contacted.

Homeroom Teacher: Students Name:

Reviewed by:

Shirin Bagchi- Head of Secondary Department

Date of Review: April 2022

Next Review Due: August 2024