Beaconhouse Private School Al Ain

E-SAFETY ACCEPTABLE USE POLICY 2025-2026

(Reviewed in August 2025)

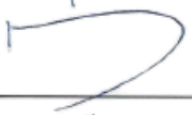
Reviewed by:	SLT
Review Date:	August 2025
Next Review Date:	June 2026
SLT's Signature:	
Principal's Signature:	
Board Governor's Signature:	

Table of Contents

1. Introduction:

At BPS Al Ain we believe that ICT is central to all aspects of learning for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

ICT in the 21st Century is 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, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up-to-date technologies in both the suite and classrooms. ICT is a life skill and should not be taught in isolation.

The computer science curriculum covers a wide range of resources including; web-based and mobile learning. It is also important to recognize the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Learning Platforms and Virtual Learning Environments
- Chat Rooms and Social Networking
- Blogging
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies. At Beaconhouse Private School, we understand the responsibility to educate our students on e-safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

2. Whole School Approach:

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures. This includes vigilance when children are accessing the internet at school to ensure that they do not access inappropriate websites.

All staff should be familiar with the school's policy including:

- safe use of e-mail & safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras publication of student information/photographs on the school website
- their role in providing e-safety education for students.

Staff and Parents are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy.

3. 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. We continually look for new opportunities to promote e-safety.

We provide opportunities within the Computer Science curriculum areas to teach about e-safety by:

- Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the ICT curriculum.
- Students are aware of the impact of online bullying and are taught how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)

- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- Students are taught about the risks inherent in using social media, particularly if they are contacted by people, they do not know

.

4. Managing Internet Access:

Children will have supervised access to Internet resources:

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.
- 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 parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
- Our internet access is controlled through the Fortinet FortiGate web filtering service.
- Staff and students are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to School IT, technician or member of SLT.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

4.1. Email:

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects,

be they staff based or student based, within school, between schools or international. We recognize that students need to understand how to style an email in relation to their age.

Students are introduced to email as part of the Computer Science Scheme of Work. The school gives staff their own email account, to use for all school activities. This is to minimize the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

Under no circumstances should staff contact students or parents using personal email addresses.

Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. The forwarding of chain letters is not permitted in school. Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

All students must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone. Staff must inform a member of SLT if they receive an offensive e-mail.

4.2. Publishing student's images and work:

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- On the school web site
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e., exhibition promoting the school General media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)
- Students' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

4.3. Social Networking and Personal Publishing:

We block/filter access for students to social networking sites. Students and parents will be advised that the use of social network spaces outside school is inappropriate

for primary aged. Students will be advised never to give out personal details of any kind which may identify them or their location.

5. Managing Emerging Technologies:

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- All classes have been issued with an interactive touch screen to be used for teaching and learning.

6. Responding to E-Safety Incidents/Complaints:

As a school we 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. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head of sections.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Head of section immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Students and parents will be informed of the complaint's procedure.
- Parents and students will need to work in partnership with staff to resolve issues.

7. Cyberbullying:

Cyberbullying occurs when technology is used to convey the bullying message to the victim and to those around the victim. Mobile phones are the preferred medium for these acts, and the proliferation of apps such as WhatsApp as well as app based social media platforms make it increasingly easy to spread negative messages much further than was possible before.

In addition, secondary perpetrators can readily forward and share the negative material, resulting in its rapid and widespread dissemination. The message may be viewed multiple times by a larger and more diverse audience – it could be sent to the victim's siblings, teachers, neighbours, and broader social groups.

7.1 Insights from the Child Rights Law in the UAE:

The UAE's Child Rights Law (Federal Law No. 3 of 2016) affirms that all children have the right to education and basic protection in the UAE. Bullying has always been difficult to punish. It is suggested that the increased use of technology may aid bullying. Equally, such technology may assist with tracing its source.

7.2 Preventing Cyberbullying:

It is important that we work in partnership with students and parents to educate them about Cyberbullying as part of our e-safety curriculum.

They should:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them
- Know what to do if they or someone they know are being cyber bullied.
- Report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Supporting the person being bullied:

Support shall be given in line with the behaviour policy:

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g., blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the student who they have sent messages to.

Investigating Incidents All bullying incidents should be recorded and investigated in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident.

7.3 Common types of Cyberbullying:

- Text messages —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
- Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatrooms.

- Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MS Teams or Google Classroom or any other platforms.
- Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal “own web space” sites.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

8. Working in Partnership with Parents:

Parents/Guardians are asked to read through and sign acceptable use of ICT 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)
- A partnership approach with parents will be encouraged. This includes parents’ evenings with suggestions for safe home Internet use.
- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

ICT Acceptable Use Policy – Parental Agreement

Dear Parent/ Guardian,

The use of ICT including the Internet, e-mail, learning platforms and today's mobile technologies are an integral element of learning in our school. In making this as successful and as beneficial as possible for all learners, we expect all students to act safely and responsibly when using technology both within, and outside of, the school environment. We review our E-Safety policy annually and have just updated our Acceptable Use Policy.

The enclosed ICT Acceptable Use Policy forms part of the wider School E-Safety Policy and in association with both the school's Behaviour Management Policy and Home-School Agreement, outlines those principles we expect our students to uphold for the benefit of both themselves and the wider school community. I would therefore ask that you please read and discuss the enclosed e-Safety Acceptable Use Policy with your child and return the completed slip at the bottom of this page as soon as possible.

If you have any concerns or would like to discuss any aspect of e-Safety, please contact the school office for further guidance.

Kind regards,
Mr Matthew Edwards
Principal

ICT Acceptable Use Policy for students:

Agreement / e-Safety Rules

I will take care when using the school IT equipment and use it properly.

I will only share my user name and password with trusted adults.

I will tell an adult if I see anything that upsets me.

I will make sure that when I blog, I am responsible, polite and sensible.

I will use a safe name and not my real name on the internet.

I know I am only allowed to go on the internet if my teacher has given me permission.

I will only take a photograph or video of someone if they say it is alright.

Any messages I send will be polite.

I will not deliberately write anything which upsets other people.

I understand that the school may talk to my parent or guardian if they are worried about my use of school IT equipment.

I understand that if I do not follow these rules, I may not be allowed to use the school computer or internet for a while, even if it was done outside school.

Parent/Guardian signature ……..

We have discussed this and …….(child's name) agrees to follow the e-safety rules and to support the safe use of ICT at Beaconhouse Private School.

Parent/Guardian name ……

Parent/Guardian signature……

Class…….. Date ……..

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with a member of SLT Team.

I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head of sections.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities. I will ensure that all electronic communications with students and staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal email address, to students.

I will only use the approved, secure email system(s) for any school business.

I will not email documents giving details of students unless on a secure system.

I will ensure that personal data (such as data held on G-Drive) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorized by the Head of sections.

I will not use or install any hardware or software without permission from the School IT.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Images of students and/ or staff will only be taken with school devices, stored and used for professional purposes in line with school policy and with written consent of the parent, guardian or staff member.

Images will not be distributed outside the school network without the permission of the parent/ guardian, member of staff or head of sections.

I understand I cannot use my mobile phone to take photos of children I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head of section.
I will respect copyright and intellectual property rights. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..…….…….. Date ……..

Full name ……

Job Title ……..