Cayman Prep and High School

E-Safety and Acceptable Use Policy

Updated: November 2020
Next review: October 2021

Introduction

ICT in the 21st Century is seen as 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 technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside the classroom include:

Websites
Apps
E-mail, Instant Messaging and chat rooms
Social Media, including Facebook and Twitter
Mobile/ Smart phones with text, video and/ or web functionality
Other mobile devices including tablets and gaming devices
Online Games
Learning Platforms and Virtual Learning Environments
Blogs and Wikis
Podcasting
Video sharing
Downloading
On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Cayman Prep and High School, we understand the responsibility to educate our students on eSafety 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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the School. This can make it more difficult for the School to use technology to benefit learners.

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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, mobile devices, 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 and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Law 2017.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

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.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.
Policy breaches may also lead to criminal or civil proceedings.
For students, reference will be made to the School's student handbook.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the School are as follows:
Mr M Graver – IT Systems Administrator

Updated: November 2020
Next review: October 2021

E-Safety

As eSafety is an important aspect of strategic leadership within the school, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Senior Management and governors are updated by the Principal/eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the School's Acceptable Use Agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHCE.

Further information on e-safety can be found at www.thinkuknow.co.uk, www.digiyen.org.uk, www.netsmartzkids.org, the safety pages for Twitter, Facebook and other social networking websites.

The School does not monitor and control the use of hardware and software owned by students but not connected through the school ICT network. Advice for parents concerning 'new generation' technology and e-safety will be found in Appendix 1.

Data Protection

The School will comply with the provisions of the Data Protection Law 2017. See Data Protection Policy.

Updated: November 2020
Next review: October 2021

Appendix 1

Advice for parents regarding 'new generation' technology and e-safety

Teenagers today have greater expertise and freedom to explore the world of the internet and experience all the fantastic opportunities that the 'virtual world' affords. However, as in the real world, there are risks attached.

At Cayman Prep and High School, we have a rolling programme of information and education on cyber-technology and its use on e-safety. This has been devised to inform and educate, in order for all our young people to make informed decisions, assess the risks and keep themselves safe. This is as important on the internet as out and about on the street.

Our filtered network enables us to supervise and safeguard school computer users. However, the recent increased ownership and use of laptop computers with built-in webcams and live video facilities such as Skype and Facetime, and 'internet enabled' devices which do not need a connection to the school network, such as students' 3G/4G/5G phones, means that young people are more vulnerable, since these devices have unfiltered and unsupervised connection to the internet.

There are implications for both students and their families.

At home, families can keep computers in supervised areas. However, with the new technology, it is easier for young people to go online anywhere, at any time.

Communication takes place with parents advising them about e-Safety, and information sessions are arranged on a regular basis to keep them up-to-date with developments in technology.

Owners of new technology devices must therefore take responsibility for their use. We will continue to educate, advise and ask parents to work with us in this endeavour to enable your children to enjoy and benefit from the technology safely.

Appendix 2

Social Networking

Social networking and the use of chatrooms is ubiquitous in teenage (and younger) circles and part of adolescent culture. Cayman Prep and High School has decided to manage this development by educating students on the safe use of such websites.

We insist upon the proper and educational use of the school network. The ICT Approved Use Policy proscribes the use of chatrooms and proxy sites. Social networking sites are not to be used during lesson times, or not at all by those under the age of 13.

Monitoring will be active. In the first instance, members of staff are to remain alert to the possibility and ask any student observed to have an inappropriate site open during the school day to close it immediately.

Appendix 3

e-mail

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing e-mail

The school gives all staff & governors their own e-mail account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

Staff & governors should use their school email for all professional communication.

It is the responsibility of each account holder 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 school business

Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

The School requires a standard disclaimer to be attached to all e-mail correspondence, stating that, ‘the views expressed are not necessarily those of the school’,

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

Updated: November 2020
Next review: October 2021

E-mails created or received as part of your school job will be subject to disclosure. 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;
Students have their own individual school issued accounts using Office 365;
The forwarding of chain emails is not permitted in school;
All student e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour 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, virus checking attachments;
Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail;
Staff must inform (the IT team or line manager) if they receive an offensive e-mail;
However, 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.

Updated: November 2020
Next review: October 2021

Appendix 4

Acceptable Use Agreement / e-Safety Rules:

Students – Junior School (Reception to Year 4)

• I will only use ICT in school for school purposes
• I will only use my class e-mail address or my own school e-mail address when e-mailing
• I will only open e-mail attachments from people I know, or who my teacher has approved
• I will not tell other people my ICT passwords
• I will only open/delete my own files
• I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
• I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately
• I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
• I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
• I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
• I know that my use of ICT can be checked, and my parent/carer contacted if a member of school staff is concerned about my safety
• I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
• If I wear one, I will not use my Smart Watch during class time and it will not have any video and/or audio recording capabilities as part of the school's data protection policy
• I am aware that I need to be older than 13 to use social media apps such as Facebook, Snapchat and Instagram. I know I need to be 16 years old or older to use WhatsApp if I am registered with WhatsApp through their EU terms and conditions.

Acceptable Use Agreement:

Students - Junior School (Years 5 & 6)

• I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
• I will not download or install software on school technologies
• I will only log on to the School network, other systems and resources with my own user name and password
• I will follow the School's 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 students, teachers or others is responsible and sensible
• I will be responsible for my behaviour 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
• I am aware that when I take images of students and/or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the School
• 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 the school community into disrepute, including through uploads of images, video, sounds or texts
• I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
• 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 and/or parents
• If I wear one, I will not use my Smart Watch during class time, and it will not have any video and/or audio recording capabilities as part of the school's data protection policy

• I am aware that I need to be older than 13 to use social media apps such as Facebook, Snapchat and Instagram. I know I need to be 16 years old or older to use WhatsApp if I am registered with WhatsApp through their EU terms and conditions.

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/carer may be contacted.

Cayman Prep and High School

Dear Parent,

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂……

Parent signature (Junior School, Rec – Year 6)

We have discussed this document with ……..... *(child's name)* and we agree to follow the e-Safety rules and to support the safe use of ICT at Cayman Prep and High School.

Parent Signature ……

Form …… Date ……

Completed copies of this form should be returned to the IT Systems Administrator via the Class Teacher.

Updated: November 2020
Next review: October 2021

Appendix 5

Acceptable Use Agreement:

Students – Senior School

• I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
• I will not download or install software on school technologies
• I will only log on to the School network, other systems and resources with my own username and password
• I will follow the School's 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 students, teachers or others is responsible and sensible
• I will be responsible for my behaviour 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
• I am aware that when I take images of students and/or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
• 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 the School community into disrepute, including through uploads of images, video, sounds or texts
• I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the School community
• 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 and/or parents
• If I wear one, I will always have my Smart Watch on **flight** or **Airplane mode**. I will follow our Phone Policy of the 4 Ps Presence, Permission, Power on and Power off
• 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/carer may be contacted
• I am aware that I need to be older than 13 to use social media apps such as Facebook, Snapchat and Instagram. . I know I need to be 16 years old or older to use WhatsApp if I am registered with WhatsApp through their EU terms and conditions.

Cayman Prep and High School

Dear Parent,

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of e-Safety and know how to stay safe when using any ICT. Students are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement.

Please return the bottom section of this form which will be kept on record at the School.

✂……

Parent signature (Senior School Years 7 – 13)

We have discussed this document with …… *(child's name)* and we agree to follow the e-Safety rules and to support the safe use of ICT at Cayman Prep and High School.

Parent Signature ……

Student Signature ……..

Form …… Date ……

Completed copies of this form should be returned to the IT Systems Administrator via the Form Tutor.

Updated: November 2020
Next review: October 2021

Appendix 6

Acceptable Use Agreement / Code of Conduct:

Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy 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 policy and adhere at all times to its contents.

- I will not use the School's email / Internet / Intranet / Learning Platform and any related technologies for anything other than professional purposes or for uses deemed acceptable by the SLG or Governing Body
- 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, personal e-mail address, personal Twitter account, or any other social media link, to students
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) 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 authorised by the SLG or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the IT Department (Mr M Graver – IT Systems Administrator)
- 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, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- 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, to my Line Manager or Principal
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the School, my professional role or that of others into disrepute
- I will support and promote the School's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies
- I understand this forms part of the terms and conditions set out in my contract of employment

Cayman Prep and High School

User Signature (Staff, Governors & Visitors only)

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School.

Signature …….…….…… Date ……

Full Name ……..... (*printed*)

Job title …….

Completed copies of this form should be returned to the IT Systems Administrator (Mr M Graver).

Updated: November 2020
Next review: October 2021