

Introduction

E-Safety. While logged into the school's network at Cranleigh Abu Dhabi, age-appropriate is defined as safeguarding children in the digital world. The digital world is rapidly growing and changing, and with that, we need to ensure that, as a school, we also safeguard children when online. Cranleigh Abu Dhabi ensures that children are safeguarded in the digital world through a range of preventative measures. Children will be part of this digital world for all of their lives and throughout their educational journey. Therefore, it and the, Therefore. is Age-appropriate while logged into the school's network. It is essential that, as a school, we have systems in place to ensure children are protected and know how to keep themselves safe when exploring such a diverse and evolving area.

"The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation: technology often provides the platform that facilitates harm. A practical approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams

(Keeping Children Safe In Education, 2021)

1. What we do as a school (age-appropriate)

1.1 The Curriculum

- The Computing Department takes E-Safety seriously and has mapped out the curriculum carefully to include all aspects.
- All pupils in FS1 to Y4 receive age appropriate input regarding their e-safety and online activity from National Online Safety resources.
- All pupils Y5 and above receive detailed input on the following:
 - Maintaining a healthy online presence
 - Strategies for staying safe online
 - What to do if uncomfortable online
 - How to support peers who run into difficulties online
 - Implications of being digital natives - growing up with the internet
 - Digital Footprint Awareness
 - Impact of online presence and behaviour on future employment
 - The UAE laws for social media and what can happen if online posts are deemed unacceptable
- The MEP scheme of work is being redesigned to include activities where pupils prepare material in lessons, ensuring that every day is a safer internet day.
- Every term, the school will focus on e-safety from the GOBubble Ecadets Curriculum, and Student Digital Leaders will lead assemblies through role-play, shared posters and presentations.
- There is a Responsible Use Policy which all pupils must sign. This includes what pupils are permitted to do when logged into the school's network and what to do to remain safe.
- The BYOD scheme (YR7-YR13) has been implemented with safeguards, and parents and pupils understand that while logged into the school's network, their online activity may be monitored for their safety.
- All Teachers have access to screen monitoring software during lessons, and this is another layer of the e-safety blanket.
- The School runs parental seminars to keep the communication channels open on the topic of e-safety.

1.2 Digital Co-curricular Activities

- All co-curricular activities are an extension of the curriculum, and subsequently, the curriculum policy is followed during co-curricular activities.
- In addition to this, some activities will require pupils to access media resources from the School network. These resources will be controlled by the member of staff leading the activity and the pupils will only have access through a school device. This forms part of the Responsible Use Policy, which all pupils have to sign.

2. Monitoring Systems

Cisco ISE controls network access. All BYOD devices are identified and moved into the correct access level. Internet access is governed by the Fortigate firewall, which identifies users and directs them to the correct internet and access permissions. Access to unsuitable content is blocked based on the following:

- Website categories, such as violence, games, social media, adult content, extremism
- Application categories, such as VPN clients, online games, communications/social media software
- Apple Classroom will be used to monitor all devices during lessons. Students must, as per the RUP, be logged into their @cranleigh.ae account.

Activity is logged and available to Pastoral staff for investigation if required. Under no circumstances are pupils permitted to move between permission blocks, and these are controlled using the user accounts to add a further layer of security.

3 Pastoral Processes

At Cranleigh Abu Dhabi, we also ensure our pastoral systems include safeguarding children in the digital world and E-Safety is covered through our Moral Education Curriculum and school systems and procedures. In addition, we have regular weekly slots for year group assemblies and whole school assemblies if this topic needs to be approached or spoken about as a preventative measure. We also hold parental seminars each

E-Safety Policy

year focusing on the digital world and how parents can support and protect their children at home and learn about what is happening in school.

Reviewed by: John Burton Gow, Director of IT
Final reviewed by: Tim McConell-Wood, Vice Principal
Reviewed on: 15/06/2022
To be reviewed by: 31/08/2023