KRISHNAMURTI FOUNDATION TRUST LTD

BROCKWOOD PARK SCHOOL
E-SAFETY AND COOKIE POLICY

Last Review Date	August 2021
Policy endorsed by	The Trustees and Principal
Policy is maintained by	IT Administrator
ISI Regulatory Paragraph Number	2, 7, 9, 10
Next review date	August 2022
Review body	Principal / DSL

Introduction

Brockwood Park School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff, and encourage the use of computers in both teaching and learning. Any user of the school IT system must adhere to the Acceptable Use Agreement. However, the accessibility and global nature of the internet and mobile phone technology mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard students, we will do all that we can to enable our students and staff to stay e-safe and to satisfy our wider duty of care.

Aims and Objectives

The school aims to inculcate a safe approach to the use of e-technology and prevent cyber-bullying in all forms and to deal rapidly and effectively with it if it does occur.
Our specific objectives are:

- To have a comprehensive e-Safety Policy that is widely distributed.
- To educate all staff and students about e-safety.
- To prevent cyber-bullying.
- To have clear procedures for dealing with cyber-bullying if it occurs.

Policy Scope

The policy applies to all members of the school community who have access to the IT system, both on the premises and remotely. The e-Safety Policy applies to all use of the

internet and forms of electronic communication such as e-mail, mobile phones and social media sites. The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

Distribution

This policy will be made readily available to students and staff and to parents of existing and prospective students. Members of staff have access to this policy which is included in the Policy Section of the school's staff server area.

Role and Responsibilities

There are clear lines of responsibility for e-safety within the school. The first point of contact should be the IT Administrator, who will report to the Designated Safeguarding Lead (DSL). All members of staff are responsible for ensuring the safety of students and should report any concerns immediately to the IT Administrator, who is required to deliver an e-safety lecture to students at the beginning of each term, and any student who joins in the middle of the year. All students must know what to do if they have e-safety concerns and who to talk to; in most cases, this will be the DSL.

The IT Administrator is responsible for keeping up to date with new technologies and their uses, as well as attending relevant training. He/she will be expected to review and update the e-Safety Policy, deliver staff development and training, record incidents, report any developments and incidents to the Principal and liaise with external agencies to promote e-safety within the school community.

Students are responsible for using the school IT system and mobile devices in accordance with the school's Use of ICT Policy. Students must act safely and responsibly at all times when using the internet and/or mobile technologies. If they believe an e-safety incident has taken place involving them or another member of the school community, they must report this immediately to the IT Administrator.

All members of staff are responsible for using the school IT system and mobile devices in accordance with the school's Use of ICT Policy. All digital communications between staff and students must be professional at all times; staff is made clearly aware of what constitutes inappropriate electronic communication with students.

Security

The IT Administrator at Brockwood Park School will do all that it can to make sure that the school network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of school systems and information.

Incidents and response

Where an e-safety incident is reported to the school this matter will be treated very seriously. The school will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to the IT Administrator or DSL. Where a member of staff wishes to report an incident, they too, must contact the IT Administrator or DSL as soon as possible. Following any incident, the school will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by the Principal, in consultation with appropriate external agencies.

E-Safety Education

Students are made aware of the following dangers involved with electronic communications:

- Not all websites are safe. Many encourage viewing but might contain programs (e.g. viruses) harmful to personal or college computers.
- Being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Never arrange to meet someone alone that you have met over the internet.
- Dangers such as cybercrime, identify theft, copyright, online gambling, inappropriate advertising, phishing and or financial scams.

- Emails requesting details of passwords (especially for sensitive information such as bank details) are certainly 'phishing' and should be deleted and/or reported to the organisation from which they purport to come.
- Personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nude and semi-nude images or videos) and/or pornography or other explicit images and online bullying.
- Do not give personal information (including address or phone numbers) or images of yourself or friends to unknown people on the internet, no matter how friendly of plausible they may seem.
- Remember that information posted on the internet, especially in social networking sites, can be viewed by millions.

- Beware of internet links that come with emails in which the senders are unknown

The school endeavours to develop critical thinking skills so that students feel empowered to evaluate the reliability and purpose of information online, rather than accepting everything at face value. This will involve asking questions, checking a variety of sources, researching the origins of information and forming their own opinions and judgements.

Cookies

To make this site work properly, we sometimes place small data files called cookies on your device. Most big websites do this too.

What are cookies?

A cookie is a small text file that a website saves on your computer or mobile device when you visit the site. It enables the website to remember your actions and preferences (such as login, language, font size and other display preferences) over a period of time, so you don't have to keep re-entering them whenever you come back to the site or browse from one page to another.

How do we use cookies?

We use two types of cookies on our website: per session cookies, which are temporary cookies that remain in the cookies file of your browser until you leave the site; and persistent cookies, which remain in the cookies file of your browser for longer (although how long will depend on the lifetime of the specific cookie) . These cookies are used to store state information between visits to a site.

How to control cookies

You can control and/or delete cookies as you wish – for details, see aboutcookies.org. You can delete all cookies that are already on your computer and you can set most browsers to prevent them from being placed. If you do this, however, you may have to manually adjust some preferences every time you visit a site and some services and functionalities may not work.