



Kisimul school

Student E-Safety Policy and Procedure

Introduction

Kisimul School recognises its commitment to improving the experience of its pupils and acknowledges the benefits of modern technology. Use of the Internet and other IT based tools has become an integral part of modern society. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Kisimul School has made a significant investment both financially and physically to ensure these technologies are available to all learners. Kisimul feel that such tools should be accessible to our pupils, as the benefits of using IT 'outweigh the risks'.

However, in its commitment to ensure that all pupils have access to the Internet in a safe and regulated manner, Kisimul Group has produced this policy as guidance and reference for our staff when ensuring the safe use of this growing and expanding technology.

The E-Safety Policy is part of the School Development Plan and relates to other policies, including: Child Protection and Safeguarding Policy; Computing Policy; Anti-Bullying Policy; Sex and Relationships Policy; PSHE and Citizenship Policy.

Risks

Whilst computers can be a fun and exciting tool for pupils and young adults they can also pose many risks.

Without responsible care, risks can include:

- Inappropriate exposure to violent and sexually explicit images or material
- Exposure to materials that could link to extremism or terrorism
- Solicitation by sexual predators in chat-rooms and by email
- Online bullying or harassment
- Piracy and illegal downloads of software, music, movies and video
- Identity theft – via disclosure of personal information

Use of the internet

The internet hosts many fantastic websites which can be used to assist learning opportunities, support research, play online games and grant access to many other great resources. However, internet content cannot always be relied upon

to be legal, decent, truthful and honest. Some information available via the Internet is highly offensive and therefore Kisimul takes all reasonable precautions to ensure the users access only appropriate material. For these reasons staff and students must adhere to the following guidelines:

- Many young people will be supervised by a member of staff at all times when using the Kisimul Internet. However in some cases, children will have unsupervised time to use the Kisimul Internet, so that they can further develop their independence and self-regulatory behaviour. In these situations, any specific risk will be assessed and documented, on a case by case basis, and this will be recorded in the student's care plan.
- Through education the students will learn that the internet is NOT to be used to access anything illegal, or anything that someone else may find offensive. Such material includes, but is not limited to, sexually and racially offensive material and language, defamatory, libelous or abusive statements and any other material representing extreme views.
- Students will be advised that they must take particular care when copying or downloading files to protect the computers from viruses and from breaches of copyright or licence conditions.
- Students will use their personalised log in to access a PC. Please note that the use of internet and email on this account will be monitored at all times and each site has its own filtering system which includes WiFi access in place e.g. Smooth wall. Each school has the facility to apply different filters for each student e.g. in accordance to their age or level of risk.
- The responsibility of control and monitoring of the pupil account will be that of the local administrator and it will be up to them and the registered manager to ensure that safety is adhered to.
- There are internet security measures in place. It is essential that staff never ignore this facility or attempt to bypass it. This security is in place to protect the students from aforementioned risks.
- Reports on internet use will be performed. The local administrator will analyse activity on the accounts and report any attempted breaches of rules to the Registered Manager.
- Students will be educated in E-Safety (as appropriate to their ability). This education will support and enable young people to be responsible users and stay safe whilst using the internet and other communication technologies for educational, personal and recreational use. The students at Kisimul generally have SLD and ASD and significant associated communication and social interaction difficulties. This therefore, has a significant impact on their understanding and ability to relate and interact with the world around them and to other people. Therefore, students should be educated to develop self-awareness,

awareness of safety and awareness of others in relation to E-Safety and everyday situations; as part of the SRE and PSHE and Citizenship curriculums in place at Kisimul. Students should be educated to recognise (where possible) the warning signs and safety procedures to ensure they know how to effectively recognise and report any concerns in relation to IT usage. This will be delivered incrementally over time, to meet the diverse needs and abilities of the Kisimul cohort; as outlined within the SRE scheme of work, computing curriculum and PSHE curriculum.

- Guidance on E-safety will also be offered to parents / carers through materials provided.

Use of Social Networking

Social Networking (for example Facebook, Twitter, Bebo, Flickr) is allowed, but the following guidelines apply:

Users should only assist in uploading photos or videos with prior permission. If appropriate and agreed on an individual basis, children and young people will be supported to access Social Networking in line with age restriction guidelines as set out by the Social Network Provider.

Staff should seek authorisation from the Registered Manager before facilitating the use of Social Networking.

- Students will be supported to understand that people can make false profiles and pretend to be somebody else in order to make friends with them. If this person is unknown to the pupil, they should not accept their friendship. Any suspicious activity or concerns should be reported to the registered manager.
- Staff should never assist in the creation of a false profile or identity. Never pretend to be somebody else. This can have serious consequences.
- Some social networking sites have a chat facility. Staff should discourage chat to anyone that they do not know or are unable to identify.

Email

Students will be supported to:

Be suspicious of all incoming e-mail, even if they know the sender They will be advised:

Not to open unsolicited e-mails or e-mails from an unknown source

- Not to send or solicit any obscene or defamatory material
- Not to send, forward or otherwise distribute spam or chain e-mail

Guidance on the use of Skype, FaceTime, What'sApp Videocall or similar Video conferencing options

Risks

- Young people can be persuaded to take or send inappropriate images and videos of themselves which can later be used to threaten or manipulate them. Other students or staff can be videoed inadvertently whilst in the vicinity of the camera device.

As a result staff must ensure caution is used when students are using this facility by using the following guidelines:

- All Video Conferencing sessions must be authorised
- Make sure the session has an allotted time and duration
- If the pupil becomes distressed/agitated or challenging staff may need to politely end the session and disconnect the link
- Following any disconnection of a session staff should ensure that they contact via telephone the participants of the session to inform them of the circumstances and any subsequent events.
- The purpose of the video conferencing session is for the young person to have contact with his/her family many students will need staff support to do this ,under no circumstances should staff be discussing any concerns with family members during the session.
- If you are unsure, or if you come across anything you feel is inappropriate, you should inform the registered manager.

Action

Despite the rigour of the approaches described above there may still be occasions where misuse of the network or other electronic media occurs. In most cases this will be dealt with by the registered manager however for more serious incidents or persistent concerns will be reported to the Kisimul Leadership team who will decide upon the most appropriate course of action.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

Cruckton Hall is a subsidiary of Kisimul Holdings Limited and as such will adopt relevant policies, where appropriate, from Kisimul Group.

Doc Ref:	Issue No:	Issue Date:	Originator:	Authorised By:
OPED 51	8	May 2017	Tjerk de Haan	Margaret Hill