INTERNET SAFETY POLICY

INTRODUCTION

Kimichi School recognises the need to maintain a strategy for effective use of the Internet as a valuable tool for learning. It also recognises the need to protect users, in particular young people, from offensive and dangerous material and acknowledges the need to ensure that all users make responsible use of the Internet.

THE FOLLOWING ACTIVITIES ARE STRICTLY PROHIBITED: Use of the Internet to harass, offend or bully any other person; Use of the Internet for any inappropriate or illegal purpose; Use of the Internet for transmission or reception of threatening or obscene material; Use of the Internet for transmission or reception of material from any criminal organisation; Use of the Internet for the transmission or reception of viruses or unlicensed software;

Use of the Internet for any personal, commercial purpose or profit. The “Use of the Internet‟ also implies the use of personal devices or other internet capable mobile communication devices in schools.

Responsibility

The school should designate a senior member of staff as responsible for student safety and security policies related to the Internet and electronic communications. The designated person along with the Network Administrator should ensure that policies are implemented and that regular monitoring takes place. Pupils are expected to sign into the Student WLAN when at school and allowed data devices to ensure safety; the firewall in place prohibits access to any inappropriate sites. The Network Administrator is able to see who is logged on thereby ensuring that private phone/tablet data is not used. All staff, including temporary and student teachers, should be made aware of policies. All users should be encouraged to use computers and the Internet responsibly and to understand the consequences their actions could have on themselves and others.

Supervision

Staff should supervise indirectly, but still be aware of learner’s access and monitor their use (through the firewall).   When parents/carers enrol children the School must ask parents to “give consent to their son/daughter having Internet access”, but parents have the right to withdraw their permission at any time.

Acceptable Use Policy (AUP)

Learners, parents/carers, staff and any other adults with Internet access must sign an Acceptable Use Policy Agreement attached to the Parent Pack sent out to all new admissions. Such an agreement makes everyone aware of their responsibilities when using the Internet. Younger children, who will not understand the AUP, should not be expected to sign but parents/carers need to know what is expected of their children and to give permission for their children to use the Internet. Parental permission only has to be given once for the whole of a child’s stay in one school but parents have the right to withdraw their permission at any time.

Personal devices

All pupils including sixth form are allowed to bring personal mobile devices to school, but must place them in the boxes allocated to them. Should they require their device, they may ask any member of staff who will decide whether this should be allowed.

Use of the Internet

The Internet can be a rich educational resource, providing access to millions of pages of information. However, much of the Internet is unorganised and unregulated and many sites contain information, which is inaccurate, dangerous, illegal or pornographic. Schools must ensure that learners do not have bad experiences when using the Internet or other forms of electronic communication and that parents have confidence that schools are using “all due diligence‟ to protect their children. Above all, we want to avoid users being exposed to offensive materials – illegal, pornographic, violent, or racist.

Child Protection

The most serious risk to learners involves the possibility of someone being hurt, exploited or abused as a result of personal information being posted online. Online pictures, names, addresses, or age can be used to trace, contact and meet a student with the intention of causing harm. Appropriate safeguarding must be followed in instances where unacceptable use has raised child protection issues, so that effective action can be taken. The potential dangers should not deter teachers and tutors from allowing learners to use the Internet as the educational advantages far outweigh the disadvantages. By following some simple guidelines and using common sense, teachers and tutors can ensure that learners can work safely online. The following internet procedures must be followed by all users to ensure safe and responsible use of the web. It should always be remembered that visits to sites are recorded and can be traced back to the user. Inform the person in charge, immediately if any abusive, threatening or offensive sites are discovered. Young children should be restricted to specific approved sites. Care should be taken that any material published to the web does not breach any of the guidelines in this policy or other policies relating to data protection, copyright and Intellectual Property Rights (IPR). Personal information should never be divulged. Use of an adult's credit card details should not take place on education premises.

Use of E-mail

The following procedures must be followed by all users to ensure safe and responsible use of e-mail. It should be remembered that e-mails are recorded, can be traced back to the sender and can be legally binding. Conceal access passwords and change the passwords regularly. Inform the teacher, or ICT Manager immediately if any abusive, threatening or offensive e- mails are received. Inform the teacher, or ICT Manager immediately if an e-mail or attachment generates a virus warning.

Staff use of e-mail

Staff may make personal use of the school Internet and e-mail facilities outside the normal teaching day. Personal use is subject to the same rules that apply at other times.

Use of Photos

Parents should be aware that they will be asked to sign an agreement letting the School use photos or videos of students where this may be deemed necessary as part of school activities.

Data Protection Act 1998 Internet Responsible Use Agreement

Staff should be aware that their e-mail is filtered and no school e-mail accounts are private. The contents of student or staff e-mail accounts or details of online activity may be checked at any time. Staff should never use school Internet and e-mail to send private confidential information or provide credit card details. Staff should be aware that their e-mail use and internet activity is monitored. Teachers should use their professional judgement in responding to texts/messages from pupils outside of school – where an issue is raised that is messaged instead of spoken, they should act accordingly.

Use of Instant Messaging – Facebook, Snapchat, WhatsApp, MSN

Many pupils use this extensively at home and are very familiar with this method of making instant communication with their friends. These are not to be accessed from school

Data Protection: Personal information about other users should never be revealed over the Internet.

Virus Protection: All computers used for access to the Internet must have anti-virus software installed. This software must be regularly updated to take account of the ever growing number of viruses. Introducing viruses to computers, or attempting to break through network security is a serious offence, and schools should be aware of the issues and the risks.   Any user who suspects the presence of a computer virus must alert the IT Manager or other responsible person immediately.

This policy agreed on (date) 29th June 2023

By

(name) Kirstie Berry

(position) Chair of Governors

Review date 29th June 2024