KILGRASTON

Pupil Acceptable Use of ICT Facilities Policy

Statement of Intent
Kilgraston believes that the internet is a resource that the school and pupils should positively engage with. Notwithstanding the recognised dangers, the internet is a net benefit to education and our policies are biased in favour of its use.

The School believes that there is no simple technological solution to the problem of keeping children safe online. One factor in internet safety is to ensure appropriate supervision. All the staff in the school are aware of the issues surrounding internet access and the need for appropriate supervision.

Major educational agencies believe that aggressive internet filtering is detrimental to the experience of using the internet in the classroom and has a limiting effect on a child's ability to use new technologies safely. As a result, our policy and practice is based around a combination of:

- A clear Acceptable Use Policy
- Technical safeguards
- Monitored usage
- Disciplinary measures

Every attempt should be made for staff, parents and pupils to work together so that use of the Internet is as safe as possible. All equipment and other users should be treated with respect and the facilities should be used in such a way that does not disrupt its use by others.

Further reading: The Safe Use of New Technologies, Ofsted
https://www.foundationonline.org.uk/course_files/safeguarding_2014/2_safer-organisations/content/documents/the_safe_use_of_technology.pdf

The Child Exploitation and Online Protection Centre (CEOP) has led on the creation of UKCCIS advice on child internet safety

Parental Role

Parents have a responsibility to be aware that there may be risks associated with Internet access and the steps the school is taking to address these. The school will do all it can to ensure that parents are informed of its Internet Acceptable Use Policy by making this document available to parents on our website.

Parents will also wish to ensure safe use of the Internet in the home or in other contexts out with school where a number of the outlined safety measures may

be absent. We strongly recommend that parents refer to available advice about safe use of the Internet and ensure that they are aware of any access that is taking place.

The School is required by law and by our Internet Service Provider's own acceptable use policy to control the activities of our users. Specifically the following legislation applies:

- The Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Copyright, Designs and Patents Act (1988)
- Data Protection Act (2018)
- General Data Protection Regulation (GDPR) (2016)
- Communications act (2003)
- All relevant child protection legislation

Any incidents involving inappropriate internet use outside school hours are the responsibility of the parents of those pupils involved and should be referred to the Police if necessary.

Further Reading: CEOP https://www.ceop.police.uk

Remit

The school will make best efforts to protect children using the internet through the school's internet connection.
The school cannot control internet access by pupils using their own devices with separate internet access (for example, 3G/4G mobile phones). However, the school does regard any access of inappropriate material on school property or during school hours to be a disciplinary matter.

Acceptable Use

Pupils and staff may use the School network for educational purposes during the school day. Educational purposes are defined as:

- Teaching
- Research
- Personal educational development
- Administration and management of courses and the educational policy of the school
- Development work associated with any of the above

Out with the school day – All usage allowed provided it does not conflict with the 'Unacceptable Use' section.

Unacceptable Use

Unacceptable use includes all of the following:

- Disclosure of usernames and passwords .The exception to this is the disclosure of passwords to the ICT Manager for purposes of troubleshooting.
- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of material with the intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of material such that this infringes the copyright of another person.
- Creation or transmission of unsolicited bulk or marketing material to users inside or outside the school.
- Deliberate unauthorised access to networked facilities or services.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    - wasting staff effort or networked resources;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - denying service to other users (for example, by deliberate or reckless overloading or damaging of equipment);
    - continuing to use an item of networking software or hardware after the School has requested that use cease ;
    - other misuse of the School network or networked resources, such as the introduction of "viruses" or other harmful software.
- The AUP covers both the schools network and any site being accessed through it. It is also expected that users will comply with any additional policy of other sites.

This means that:

- Email addresses should only be passed to trusted individuals.
- Any email from unknown sources should be reported.
- Any person who believes that attempts have been made to make unacceptable use of the Internet should report the matter immediately to the Headmistress, the Head of Pastoral Care and Boarding, the Head of Junior Years or the ICT Manager
- Any person who discovers any materials they consider may be offensive or inappropriate should report the matter immediately to the Headmistress, the Head of Pastoral Care and Boarding, or the ICT Manager.

- Any material viewed or printed off the Web or through other electronic means should not contain any offensive material and should be checked by a member of staff before being made publicly available.
- Users should be cautious about using their home address or phone number when on the network, if in doubt ask.
- On sites where photographs and video clips of pupils may be uploaded, users should not disclose pupil's full names or other personal information.
- Users should be aware that internet access is monitored and that every site they visit is recorded and may be traced back to them.
- The school reserves the right to restrict or remove access in the event of any user misusing network and ICT facilities.
- As well as these, a number of aspects are under strict control of the classroom teacher:
    - The use of chat and newsgroups is restricted. Any use of these facilities should be in line with specific instructions issued by the class teacher.
    - Saving or downloading materials is subject to guidance from the class teacher.
    - Materials saved or downloaded from the Internet must not infringe copyright.
    - Pupils may not use disks/CDs brought from out with the school without prior permission.
- Pupils must not attempt to circumvent any security or restriction settings applied to school computers or networks.

Use of Wi-Fi Network

Pupils may access the school WiFi network on any devices. Any device used for accessing the WiFi is bound by this policy.

Use of iPads

Class set of iPads, to be kept in class and used under teacher supervision.

Use of Mobile Phones & Personal iPads

Mobile phones & personal iPads:

- are not permitted for use in lessons or activities.
- should be given to the Welfare team in accordance with our Mobile Phones Policy
- must not be used to listen to music during any lessons or activities

If the use of a phone is required in the case of an emergency, girls must seek the relevant manager's permission, or use the Reception phone.

Pupils found breaking the school rules regarding the use of mobile phones during the school day, and/or accessing inappropriate materials, are at risk of

these being taken from them for the duration of the school day. If deemed necessary they may be banned from having them in school. Additional formal action may also be taken as is appropriate i.e. detention

Cameras

Pupils should not use cameras (including cameras built into mobile phones and iPads) in school without the permission of a member of staff.

If taking a photo of another student, they should ensure they have the other student's permission to do so.

Audio/Video Recording

Pupils should not use recording equipment (video or audio) without the permission of a teacher and the permission of the people being recorded. Under no circumstance should covert (hidden) recordings be made.

Responsible Persons

The Summer School Course Director, Senior Leadership Team, Director of Studies, Activities Manager, Welfare Manager, and the ICT Manager are the designated members of staff assigned to oversee the use of the Internet in Teaching and Learning and to ensure it is used safely and securely.
Child Protection and all safety are also part of the remit of every staff member.

Disciplinary Measures

Pupils found in contravention of this Acceptable Use Policy may be subject to measures including, but not limited to:

- Detention
- Withdrawal of access to the network
- Withdrawal of access to computer use in school
- Mandatory check in of pupils' own devices in accordance with the Mobile Phones Policy
- Parental involvement
- Temporary or permanent exclusion from school
- Police involvement

Updated 16/01/2020 D MacGinty
Updated 07/09/2020 D MacGinty
Updated for Summer School 30/09/2020 D Douglas