INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

Date: September 2015
Compiled: S Kirk
Revised: 16/02/2016
Edited: R Malcolm

Preamble:
This policy applies to all users of the Bridge House network.

Definitions:
This policy applies to all digital devices, including but not limited to “smart devices” including tablets, cellular phones, laptops and desktop computers. This includes devices of a similar nature that may come onto the market in the future.

Expectations:
Pupils are responsible for appropriate behaviour on the Internet just as they are in a classroom or sports field. Communications on the Internet are often public in nature and general school rules for behaviour and communications will therefore apply. Pupils are personally responsible for their actions in accessing and utilising the school’s information technology resources. Pupils are advised never to access, keep or send anything that they would not want their parents or teachers to see. It is expected that users will comply with the standards and rules set out below.

Specifically-acceptable uses:
There are limitations on our use of the Internet. All traffic downloading or uploading information to or from our network attracts costs which are borne by the school. Students are expected to use this resource for:

- direct educational purposes;
- accessing information for private appropriate interests or hobbies;
- constructive communication with other Internet users including, but not limited to, Bridge House students and members of staff;
• downloading of Apps from the Apple App Store, that are to be used for educational purposes.

Specifically-unacceptable uses:

Users are not to:

• take part in the sending or re-sending of any sort of chain letters;
• make use of Internet Relay Chat (IRC) and "Chatrooms";
• use offensive language or language which may be deemed offensive in any written communication over the Internet;
• attempt to access or create any sort of pornographic or sexually explicit material of any kind whatsoever, be it via E-Mail, the World-Wide-Web or any other Internet facility;
• use any other student’s E-Mail account and thereby impersonate (and incriminate) any other user; this includes changing the name of a device in order to impersonate another user.
• use any other student’s information to access social media;
• use any other individual’s information to create fraudulent profiles on any website, messaging service or social media platform;
• use any other student’s access codes to perform unauthorised modification in any form to any other student’s personal device;
• insult, bully, threaten or abuse any other person via any platform whatsoever.
• use messaging services on mobile devices for activities that are disruptive to academic practices or which are hurtful or discriminatory;
• use facilities such as AirDrop and AirPlay inappropriately;
• attempt to bypass the schools’ firewall or gain unauthorised access to the schools’ internet connection;
• attempt to gain unauthorised access to servers or other network resources;
• vandalise any data or equipment.
Use of the school’s internal computer network:

IT Users must note the following:

- All users are entitled to privacy of their work and communication and therefore it is an offence to use or attempt to use another user’s account/password no matter what the circumstances may be.

- Storage capacity is at a premium and pupils are to conserve space by deleting unnecessary email or other material which takes up excessive storage space.

- Pupils should never download or install any software onto network drives. All copyright rules must, therefore, be obeyed. Students should not attempt to install or run any software not already installed on the device that is being used.

- Pupils have full responsibility for their accounts and must not share their passwords with anyone, and therefore, any violations of any part of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account.

- Pupils have full responsibility for the information contained on and broadcast by their personal devices, including their iPads. Pupils are to keep their passcode, Apple ID passwords and other login details strictly confidential. All devices are traceable on the school’s network and students will be held responsible for any illicit activities performed on their device.

- Participation in any kind of P2P file-sharing service is not permitted. (E.g. Downloading of films, videos, music)

- Bridge House operates a strictly-controlled firewall to ensure the safety of all users of the school’s network. Any attempts to bypass, deactivate, disable or damage this service will result in disciplinary measures being taken.

Use of cellular devices:

A cellular device is defined as any device which makes use of a cellular telecommunications network to gain access to voice and data services. This term includes, but is not limited to, cellular phones, iPads with cellular (3G or LTE) connectivity and portable Wi-Fi hotspots which use SIM cards.
While the school cannot control the use of cellular devices, it is important that all users are aware of the following:

Any student who is found to be accessing content that is inappropriate will face disciplinary actions in terms of the school’s Code of Conduct.

- Such content includes, but is not limited to:
  - pornographic or sexually explicit material;
  - material that contains graphic violence;
  - material that contains explicit or defamatory lyrics or writing;
  - material that encourages or promotes discrimination of any kind;
  - material that can be used to humiliate another person;
  - material that has an age restriction older than the user’s age.

- Students should also be aware that using cellular devices to bypass the school’s firewall and access information that is considered inappropriate, is not permitted.

**Gaming:**

Gaming can be used for constructive educational purposes. However it can also have an addictive element that can waste significant amounts of time, can be anti-social and can hamper holistic development. Gaming may not:

- infringe on the rights of others and may not cause offence to others;
- reduce others’ access to the network;
- encourage violence and anti-social behaviour.

**User Accounts:**

Old user accounts will be deleted each holiday period. Each account will be kept live for a minimum of one month after the user leaves the school. It is the user’s responsibility to remove any personal information from the school’s network during this period. In certain cases a disciplinary hearing may require the immediate shut down of a specific account. Personal information that has not been backed up may be lost in this situation.
Consequences:

Should there be reasonable suspicion that unacceptable use has occurred, the school reserves the right to view any data stored on digital devices on the school’s premises. Similarly the school reserves the right to view any data stored in user accounts on the school network.

The school’s Code of Conduct and Disciplinary Procedures Guidelines will apply should transgressions of this policy occur.