CAMBRIDGE HOUSE GRAMMAR SCHOOL

INTERNET POLICY

Code of Practice for safe and effective use including, Bring Your Own Devices (BTOD)

Introduction
This document has been drawn up in conjunction with the DENI Circular 'Acceptable Use of The Internet' and the e-Safety Guidance 2013/25. It takes account of the C2K provision for and the impact of the 'Empowering Schools' document on school provision.
When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web- based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed we must consider ICT a life- skill. Most technologies present risks as well as benefits and internet use brings young people into contact with a wide variety of information, some of which could be unsuitable.

1 The purpose of the Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
2 Internet use is a part of the statutory curriculum and a necessary tool for both pupils and staff.
3 Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
4 The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
5 Benefits of using the Internet in education include:
- Access to world-wide educational resources, including museums and art galleries;
- Inclusion in government initiatives such as the National Grid for Learning (NGfl),LNI, Frontier, distance learning providers and the use of Virtual Learning Tools;
- Educational and cultural exchanges between pupils world- wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and sound curriculum practice;
- Communication with support services, professional associations and colleagues.

Responsibility
Internet safety depends on staff, school, governors, advisers, parents and, where appropriate, pupils themselves taking responsibility for the use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully. School access is denied for unmoderated chat rooms, gaming areas or areas of inappropriate material. Fair rules, clarified by discussion and prominently displayed will help pupils make responsible decisions. At home, parents should reinforce such restrictions by discussing eSafety with their children and checkings upon sites accessed by their children; inappropriate use of internet, e-mail connection between home and school affecting other pupils in school may be regarded as a breach of school rules on the appropriate use of the internet. Parents are advised to supervise their child's use of the internet at home at all times. School cannot accept absolute responsibility for pupil behaviours, while under the understood supervision of parents off the school site.

Appropriate Strategies
This document provides strategies to help ensure responsible and safe use of the Internet within school. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the pupil in question, the school situation and their effectiveness. This is monitored on an annual basis. There is no right answer to an effective solution for this developing technology. Staff, parents and pupils must remain vigilant to ensure safety of access and use.

1 Staff and Pupils :
- The school Internet access has been designed by C2K expressly for pupil use and includes a high level of filtering appropriate to the age of the pupils;
- Staff are allocated filtered e-mail for professional use and must be aware that **all filtered items are held by C2K and can be viewed by the Principa**l. Where required other e-mail can also be viewed by the Principal or designated member of staff. Staff must not bring the school name into disrepute on social media, websites, or other electronic communication forums;
- Pupils are allocated filtered e-mail facilities through the C2K system; they should be aware that the same procedures for access to staff e-mails are in place for pupils;
- Pupils will be provided with what are acceptable and what are not acceptable procedures for Internet use;
- Internet access levels will be reflected in the curriculum requirements and age of pupils;
- Staff will guide pupils in on-line activities which will support learning outcomes planned for pupil age and maturity;
- Pupils will be educated in the effective use of the Internet in research, e-communication and e-learning. This will be conducted through both subject and pastoral systems. Monitoring of this will be carried out by Middle Leaders and SLT staff;
- Teachers and support staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector. Breach of such standards of conduct will result in disciplinary action.

- Pupils are responsible for their good behaviour on the school networks, just as communication technologies is a required aspect of the statutory Northern Ireland Curriculum, **access to the Internet and to C2K is privilege and not a right**. This access for Cambridge House pupils is given to those who act in a considerate and responsible manner and **will be withdrawn** if pupils fail to maintain acceptable standards of use.

Staff should ensure that pupils know and understand that no Internet user is permitted to:

- retrieve, send, copy or display offensive messages or pictures;
- use obscene or racist language;
- harass, insult or attack others;
- damage computers, computer systems or computer networks;
- violate copyright laws;
- use another user's password;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as on-line time and consumables);
- use the network for unapproved commercial purposes.

2 Location and Supervision

(a) The school will provide through an Internet Service Provider, a filtered service. All users should be aware that the school can and does track and record the sites visited, the searches made on the Internet and e-mail sent and received by individual users.

(b) While using the Internet at school, pupils should, where possible, be supervised. However, when appropriate pupils may pursue electronic research independent of staff supervision if they have been granted permission. In all cases, pupils should be reminded of their responsibility to use these resources in line with school policy on acceptable use.

(c) The school will endeavour to ensure that all pupils understand how they are to use the Internet appropriately and why the rules exist. Lessons on internet usage are taught within the pastoral programme.

(d) The network administrators may view files and communications to maintain the system and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on C2K servers to be absolutely private.

3 Examples of Acceptable and Unacceptable Use:

(a) On-line activities which are encouraged include, for example: the use of e-mail and computer conferencing for communication between colleagues, between pupil(s) and teacher(s), and between pupil(s) and pupil(s), between schools and industry; use of the Internet to investigate and research school subjects, cross-curricular themes and topics related to social and personal development; use of the Internet to investigate careers and Further and Higher Education; the development of pupils' competence in ICT skills and their general research skills.

(b) On-line activities which are not permitted include, for example:

- Searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- Copying, saving and/or redistributing copyright protected material, without approval;
- Subscribing to any services or ordering any goods or services, unless approved by the principal;
- Playing computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher;
- Using the network in such a way that use of the network by other users is disrupted (example: downloading large files during peak usage times; sending mass e-mail messages);
- Publishing, sharing or distributing any personal information about a user (such as: home address; phone number, etc.);
- Any activity that violates a school rule.

(c) **Cyber Bullying: (Reference to CHGS Anti-Bullying and E-Safety Policies)**

Staff should be aware that pupils may be subjected to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is referred to in the Anti-Bullying Policy and the e-Safety Policy.
Care should be taken when making use of the social media for teaching and learning. Each social media technology that is to be utilised must be risk assessed in the context of school use.

Cyber Bullying can take many different forms and guises including:

- E-mail- nasty or abusive which may include viruses or inappropriate content;
- Instant Messaging (IM) and Chat Rooms- potential to transmit threatening or abusive messages perhaps using a compromised or alias identity;
- Social Networking Sites- typically includes the posting or publication of nasty or upsetting comments on another user's profile;
- On-line gaming- abuse or harassment of someone using online multi-player gaming sites;
- Mobile Phones- examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people;
- Abusing Personal Information- may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils must be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection form Harassment (NI) Order 1997
- Malicious Communications (NI) Order 1988
- The Communications Act 2003

Pupils must report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure that the matter is properly addressed and the behaviour ceases.

As part of the pastoral records all cyber-bullying incidents will be recorded to monitor the effectiveness of the preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

4 Advice for Parents:

(a) While in school teachers will guide pupils toward appropriate materials on the Internet. Outside school, parents or guardians bear the same responsibility for such guidance as they would normally exercise with information sources such as television, telephones, movies, radio or other media.

(b) Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and schoolwork. It should, however, be supervised, and parents should be aware that they are absolutely responsible for their children's use of Internet resources at home.

(c) Offering advice to parents is good practice and Cambridge House therefore advise parents that it provides filtered and monitored access to the Internet for pupils and draw attention to the advice and guidance contained in this policy for its use within the home environment.

(d) The following guidelines are proposed in the first instance:

- Parents should discuss with their children the rules for using the Internet and decide together when, how long, and what comprises appropriate use;
- Parents should get to know the sites their children visit, and talk to them about what they are learning;
- Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way parents can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud;
- Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages or images. If the message comes from an Internet service connection provided by the school, they should immediately inform the school.
- Parents should report any obscene, threatening, sectarian, hate-related, abusive or malicious e-mail, text or message to the PSNI who will investigate every offence reported to them.

Bring Your Own Devices (BYOD)

The School recognises that as technology has changed more pupils have access to Internet capable devices. This should be seen as a resource and provide an opportunity to enable quick and easy access to the Internet to enhance learning. Devices in the form of mobile phones, music players and tablet computers should no longer be looked on as distractions or contraband but should be used in classrooms to aid learning when short bursts of activity are required and a mobile device is more appropriate than a laptop or desktop computer.

General Information

Access to Cambridge House wireless network, whether with school-provided or personal devices, is filtered in compliance with the Children's Internet Protection Act (CIPA). However, access from personal devices is limited to Internet use only. Pupils will not have access to any documents which reside on the school network from their personal devices.

Access to Cambridge House wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and an absolute compliance with all school rules. The use of the network also allows IT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request.

Obtaining access to the wireless network:

There are two stages to connecting to the wireless network. Authenticating the device and then authenticating the session. The first stage is only required on first connection and involves authenticating and then downloading a small applet called Smart Connect, which configures the connection to the C2k network.

For personal devices: a user should authenticate using their own C2K user name and password.

1. On your device, locate and connect to the C2kGuest wireless network.
2. Launch the browser.
3. Read and Accept the Terms and Conditions set out in the Acceptable Use Policy.
4. For personal devices, when prompted, enter your C2k username and password.
5. Download and install SmartConnect: instructions for download and install may vary by device/browser.
6. Return to your browser and enter your C2k username and password when prompted (with your username prefixed by 'c2ken\', e.g. c2ken\jbloggs 123. You may need to attempt to browse to a website first in order to be prompted.
7. You should now be connected to the C2k guest wireless network and able to access the internet.

Note: Items 3 and 4 are only required the first time a device is connected to the C2k Guest Wireless Network.

Guidelines for use:

- Use of personal devices during the school day is at the discretion of staff. Pupils must use devices as directed by staff;
- The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. contacting parents, should only take place after permission has been given from a teacher or other member of staff;
- The use of a personal device is not to be disruptive to teachers or pupils. Personal devices must not disrupt a class in any way;
- The use of personal devices is incorporated into Cambridge House's Acceptable Use of the Internet Policy. This is found on the School website. A summary of the rules for Internet use is emailed to all staff and pupils each time it is updated. The policy is provided in hard copy to all new pupils from September 2014; this includes an agreement for appropriate use as described within the policy. All pupils (Years 9-14), enrolled in the school, will re-new their agreement in September 2014.
- Pupils will not use personal devices outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities;
- Pupils shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security;
- Pupils shall not distribute pictures or videos of pupils or staff without their permission (distribution can be as small as emailing/texting to one person or as large as posting image or video online).

Consequences for Misuse/Disruption:

(One or more may apply)

- Access to the wireless network will be removed;
- Device taken away for a period;
- Device taken away and retained in the main office until collected by a parent/guardian;
- Pupil not permitted to use personal devices on the school premises or during any off site school activities.

Misuse of Internet capable devices is regarded as a serious offence within the School's Discipline Policy and will be dealt with according to this policy.

School's Liability Statement

Pupils bring their personal devices to use in Cambridge House Grammar School at their own risk. Pupils are expected to act responsibly with regards their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Cambridge House Grammar School is in no way responsible for:

- Personal devices that are broken while at school or during school-sponsored activities;
- Personal devices that are lost or stolen at school or during school-sponsored activities;
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

This policy document will be reviewed annually by the SLT and Board of Governors to ensure that all aspects of Child Protection Services are being addressed as appropriate.

Signed: Margaret Thompson Chair of Board of Governors

Signed: S. C. Sutton Principal

Date 2 December 2014