Hospital and Home Education Learning Centre

ICT Acceptable Use Policy

ICT Acceptable Use Policy

1. The technologies

ICT has an all-encompassing role within the lives of the students and adults at HHELC. New technologies are enhancing communication and the sharing of information and learning opportunities. Current and emerging technologies used in school which require consideration for acceptable use are

- The Internet
- E-mail
- Digital images including the use of web cams and video cameras
- Simple messaging and blogs
- Video broadcasting sites
- Music download sites
- Mobile phones with camera and video functionality
- Storage and use of photographs/video
- Software and games to support learning
- Sensitive or confidential data

2. A whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for students, staff and parents.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The **Head Teacher** ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Co-ordinator** is **Arti Pearson**

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance *through liaison with the Local Authority* e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[1]. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are updated at least annually on policy developments.

All staff are responsible for promoting and supporting safe behaviours and following school e-Safety procedures. This includes;

- **Safe use of e-mail**
  User names and passwords should be kept secure. Email is accessible from outside home through the *learn.nottingham* portal. Email should be used for work purposes only. Staff should be aware of confidential data and information when sending/receiving emails. Mimesweeper is used to filter emails from profanity and junk emails.

- **Safe use of Internet, including use of internet-based communication services, such as instant messaging and social network**
  Staff must check all content for internet searches before working with the students. All staff members should refer to 'Personal Blogs and Websites' guidelines, which are signed by all staff members.
  The school works closely with Capita to ensure unsuitable websites are blocked. Netsweeper is used to support this. Staff are responsible for reporting any unsuitable material to Capita immediately.

- **Safe use of school network, equipment and data**
  Staff, student and class log ins have been set up to protect each user group and should be used as follows;
  - **Student log in** - students work towards their own portfolio giving them identity. It is also used as an archive of work and photos. There are restricted permissions e.g. not able to delete shared work.
  - **Class log in** - for shared class work e.g. on the Interactive White Board. Allows all class staff to access class resources, which is useful in the case of the absence of teaching staff. Permissions are increased compared to the student log in.
  - **Staff log in –** for documents staff are working on, confidential documents. Increased permissions.

  The **staff shared area** is only available to staff and contains information about students, curriculum planning and policies. Staff have access to assessment data and some staff have access to SIMs.
  The **student shared area** is available to both staff and students and should be used to **share resources**.

  Staff and students have their own user names and passwords. Classes have a shared user name and password. Passwords should be kept safe and secure.

- **Safe use of digital images and digital technologies, such as mobile phones and digital cameras**
  School owned and managed cameras are used to take photos or video of students.

  Photos of students are stored on the network. Photos of students should be archived in the students own area (my area) under their own personal log in e.g. Jane Smith 2009 2010.

- **publication of student information/photographs and use of website**
  Parents are consulted regarding the use of photographs/video for use in school and in the wider world. Staff are responsible for ensuring that students have the relevant permissions for the use of photos/video.

- **Ebullying / Cyberbullying procedures**

Staff monitor student access to the internet very closely. If a case of eBullying / Cyberbullying occurs this is referred to the E-safety co-ordinator.

- **E-Safety education for students**
  This is addressed on an individual basis and is dependent upon the students ability to access the internet independently. It is advised to work with parents and carers on this matter.
  If students are accessing the Internet, an E-safety guidelines sheet is shared with the student in order for them to understand the risks.

Staff are reminded / updated about e-Safety matters at least once a year.

4. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. For example, staff need to ensure they have checked all content for internet searches before working with the students.
However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. However, Capita must be informed immediately. Our e-Safety Coordinator acts as first point of contact for any further complaint. Any complaint about staff misuse is referred to the Head teacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Created by: David Blackley *Updated: David Blackley*

Reviewed by Chair of Governors, Judith Ward on 23/03/2017