HHELC Education
eSafety Policy

Our e–Safety Policy has been written by the HHELC ICT working party, building on the national guidance.

The policy covers all Education provision offered by HHELC including the Thorneywood Base, Hospital School and Home Tuition.

HHELC Education's Safeguarding lead takes responsibility for eSafety alongside the eSafety coordinator and eSafety working party.

As a service we have committed to the 360 degree eSafe audit as this provides an opportunity to routinely benchmark our policy and practice against the highest standards nationally in eSafety.

The School eSafety Coordinator	Arti Pearson
Policy approved by Governors (including Governor with responsibility for Safeguarding)	
Policy approved by eSafetyWorking Party	
Review by Chair of Governors	23/03/2017
Signed by Chair of Governors	Judith Ward
Date for the next policy review	March 2017

Version control

Version 1	Completed 2 October 2015
Version 2	Updated section: How will students access their on-roll school IT systems? Resolve minor punctuation errors.
Version 3	Updated section: Use of routers at QMC Jan 2016

Policy Contents

Version control
eSafety Policy
What ifs...a practical guide to dealing with eSafety issues in class.
Useful e-Safety Contacts and References
Significant Incident form sent to LM and HandS director.
eSafety long term overview, scheme of work (Draft)

eSafety Policy

Introduction

Overall vision for eSafety

Safe to learn
We want our young people to work and play thoughtfully in a safe environment whilst in our care.

Safe for life
We want our young people to live a safe digital life, harnessing the great opportunities which technology brings us whilst feeling empowered to make good choices to stay safe with technology.

What do we mean by technology?
Technology within this policy means electronic equipment which provides us with information. Technology is another word for ICT (Information and Communications Technology)
This includes the hardware, such as laptops, tablets and iPads and desktop computers and software which are the programmes and applications which people use. Examples of software programmes include Microsoft Office tools such as Word .This definition also includes the things which are harder to see, such as the internet and computer network. These are types of ICT services. Throughout the policy we may use the term technology and ICT interchangeably.

A whole school approach to the safe use of ICT
Creating an eSafe learning environment includes three main elements:
An effective range of technological tools
Policies and procedures, with clear roles and responsibilities.
A comprehensive eSafety education programme for students, staff and parents.

How does technology benefit education in HHELC?

ICT benefits learning and teaching in the following ways:

- Provides an engaging and motivational way to learn, especially for some of our most disengaged learners.
- Allows students access to a rich variety of multimodal information eg. video, audio, images, text, to engage numerous learning styles and preferences.
- Allows students to connect to learning in accessible ways eg. by providing a writing framework or having the computer read instructions to them to support various learning needs.
- Supports high quality teaching through the use of diverse and interactive resources.
- Supports a collaborative approach to learning in a managed, structured and controlled way to compliment face-to-face collaboration.
- Supports personalisation by providing flexibility in the pace, place and time of learning.
- Culturally enriching by connecting students to people and communities in different localities, opening minds and raising awareness of our cultural heritage and responsibility as global citizens.

The internet can provide the following specific benefits:

- Access to worldwide educational resources.
- Educational and cultural exchanges between students worldwide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data through our systems eg. Office 365.
- Access to learning wherever and whenever convenient.
- Communication systems with up-to-date information.

How can internet use enhance learning?

- Education can happen away from school, using tools such as Office 365.
- Internet research, including the skills of knowledge location, retrieval and evaluation.
- Online activities that support the learning outcomes planned for the students' age and ability.
- Students learn to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Resources and software used in school are accessible from home.

Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Copyright law will be adhered to by the school when using materials from the Internet.

Commitment of HHELC Education to eSafety

We are committed to improving our approaches to eSafety and keeping staff and students safe.

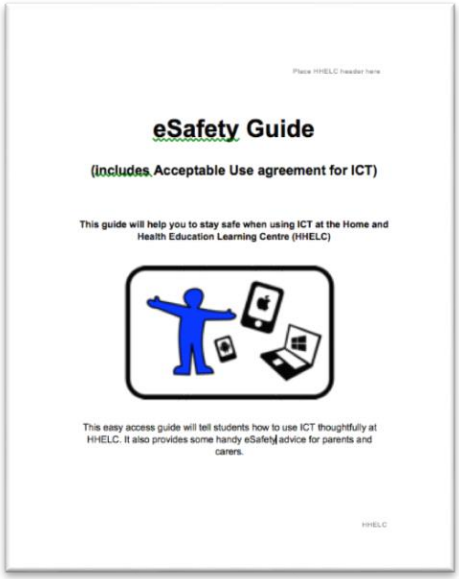
We use http://www.360safe.org.uk/ to benchmark HHELC Education against other schools nationally.

We have currently been awarded a Certificate of Commitment from the national 360 degree eSafe campaign.

HHELC.

In addition, we plan for eSafety developments through the eSafety/Safeguarding Action Plan which sets out a series of actions to improve our approach and delivery of eSafety projects and programmes in a coordinated way across HHELC. Education.

On induction at HHELC
When students are inducted at HHELC, they are asked to read and sign our **eSafety Guide** (A visual Acceptable Use form). This is their contract with us to ensure they take their responsibilities for eSafety seriously and that their parents/carers will do likewise to support us.


eSafety Guide

(includes Acceptable Use agreement for ICT)

This guide will help you to stay safe when using ICT at the Home and Health Education Learning Centre (HHELC)

This easy access guide will tell students how to use ICT thoughtfully at HHELC. It also provides some handy eSafety advice for parents and carers.


Advice to stay safe when using ICT

ICT stands for Information Communication Technology. Laptops, ipads, tablets, mobile phones and desktop PCs are all types of ICT.

The internet and websites are ICT too.

We use ICT at HHELC to help us with our learning.

Always ask an adult if you want to use ICT. Ask an adult if you want to send a message to someone using ICT.

Be nice to other people when using ICT because you don't want other people to feel sad. If someone is being nasty to you tell an adult you trust.

The agreement needs to be printed out, signed and completed, a copy provided for the parent/carer and students (as appropriate) to take home with them. A copy should then be returned to the central students file for future reference.

Managing Information Systems

How will information systems security be maintained?

- Updating virus protection regularly.
- Activation of proactive and reactive systems to manage threats including the use of Netsweeper, mail filtering and anti-virus protection.
- Regularly assessing access to a learners information through during key milestones eg. person centred planning meetings.
- The ICT technical support service will regularly review security procedures
- User logins and passwords are required to access confidential data.
- Personal data sent over the Internet, stored in Office 365 or taken off site will be encrypted.
- Regular, planned training and support for all staff who access information systems including regular eSafety updates and training for all staff.

How will email be managed?

- Staff have access to email, their responsibility is clearly identified in our acceptable use policy which is signed on induction by all staff.
- Students use of email is permitted with the Headteacher's consent and restricted to email within HHELC. (ie. the students cannot email someone who does not have an @hhe.nottingham email address without prior permission from QMC or TEB Head.)
- Students's agree to acceptable use policy.
- Email security and filtering is monitored and maintained by the ICT technical support service.

How will social networking, social media and personal publishing be managed?

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured to stop students accessing personal information about them and how publishing unsuitable material may affect their professional status at HHELC Education.

In different industries, there are varying expectations around the use of social media eg. Facebook, Twitter and Linkd In. As HHELC is a school, we set very high standards around responsible use of social media. This includes the use of social media in non-work time for personal use that would reflect negatively on HHELC.

All staff have a responsibility to ensure their actions when using social media do not compromise the integrity and professional standing of themselves and HHELC Education.

As internet sites and resources are increasingly adding a social element to their appearance and operation, staff should consider all web resources carefully.

Students use of social media

- Where filtering is in operation, access to social media and social networking sites can be controlled (or blocked) by filtering software.

- Social Media tools used in the classroom will be risk assessed before use and planned into a scheme of work with agreement from Headteacher prior to the lesson.
- Students will be advised on security and privacy online and concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Students will be advised never to give out personal details of any kind which may identify them and/or their location (as agreed at induction).

Staff use of social media

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.
- Staff should not use social media to "sound off" about their day or staff/children. Social media to share anonymised teaching and learning experiences e.g. discussing resources and strategies used, is acceptable. Opinions should not relate to the school or allow a child to be identified in any way.
- As a general rule, staff should refuse any contact from young people they teach or have taught or parents (current and past) through social media.
- A good rule of thumb is to consider; How would my Headteacher feel if this message/post was read by them?

An excellent guide for staff who use Social Media in both professional and personal life should be read: http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals

How will filtering be managed?

- Broadband access includes filtering appropriate to the age and maturity of students and the school's filtering policy will be regularly reviewed by the eSafety working party, with changes being risk assessed and with consent from the Headteacher where appropriate.
- Any breaches of filtering (e.g. inappropriate content) will be reported to the Headteacher and logged in the eSafety log. All members of the school community (all staff and all students) will be aware of this procedure at induction.
- The eSafety working party will meet regularly to review the eSafety log and check that any necessary changes are made to ensure that the filtering methods selected are effective.
- The school's filtering decisions will pay heed to the age and curriculum requirements of the students, with advice from network managers.

Use of routers on QMC wards.

The routers can be used by any student/students as long as there is a member of staff on the ward.

Under no circumstances should a router be left unattended (staff must take the router with them when they leave the ward).

It is the staff's responsibility to ensure that pupils are not accessing inappropriate websites.

When connecting to the router you will need a password- staff must ensure that pupils/parents/other hospital staff and visitors do not have access to this password.

It is at the discretion of the individual member of staff as to who (pupils) can use the router on the wards as long as it is used for educational purposes.

Wi-Fi should not be used for any activity that incurs high Wi-Fi usage ie:

- viewing videos online e.g. Vimeo and YouTube,
- downloading or streaming music,
- accessing social media
- downloading software / apps
- installing any updates.

Unblocking websites that have been blocked by the filtering software
Occasionally, the filtering software blocks legitimate and safe websites which would add value to learning.

Where staff wish to unblock or gain access to a filtered website, they will contact the Headteacher for permission to unblock a website. Where the website is clearly safe, the ICT technician will unblock the site and record the decision for future reference. Where there are concerns about a website's safety/security, the technician will discuss concerns with the member of staff. If the request cannot be resolved, the issue or request should be raised to the Headteacher for a final decision.

How will videoconferencing be managed?

- The use of videoconferencing with children will be planned and confirmed by the Headteacher prior to use.
- Staff to refer to a crib-sheet for reminding the other party about house rules etc…
- Staff will never leave children unattended when a video conference is in progress.
- By default, all video conferencing services are restricted as default to people within the Nottingham City Local Authority.

- Staff will have access to the Office 365 video conferencing service provided to connect and communicate with each other. The use of this service is for professional use only in work and non-work time.

How are emerging technologies managed?

- Emerging technology means any new ICT innovations.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school eSafety Guide.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See also the Data Protection Policy).
- HHELC Education will comply with freedom of information requests in accordance with Freedom of Information Act 2000 and recommendations from the Information Commissioner's Office.
- HHELC Education demonstrates this compliance by registering with the Information Commissioner's Office that we process personal data.
- We have a Data Policy which outlines the full responsibilities and expectations of how we process and store data at HHELC.

How will Internet/wifi access be authorised?

- All staff will read and sign the Acceptable Use Policy at induction.
- All guests and visitors will sign and complete the above form before being given an wifi password to provide limited access to the internet. The access will be removed after a limited period of time.
- Parents will be asked to read and sign the **eSafety Guide** for students and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign the **AUP Acceptable use policy for visitors**
- The policy informs that students will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education or emotional needs) the school will make decisions based on the specific needs and understanding of the students(s).
- Students will be carefully supervised to access the internet or use technology.

How will risks be assessed?

- HHELC will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. HHELC cannot accept liability for the material accessed, or any

consequences resulting from internet use.

- The school's eSafety working party in conjunction with the Headteacher regularly meet and review the eSafety policy (at least annually), to ensure it is adequate and being implemented appropriately. They will identify, assess and ensure methods are in place to minimise risks.

How will students access their on-roll school IT systems?

Students may access hardware and software systems provided by their on-roll school providing

- They request permission from the Headteacher and authorisation is gained from the ICT technical support staff at HHELC via QMC and TEB Heads.
- They have gained permission to use these systems from their on-roll school.
- They are not breaking licencing terms and conditions of the software.
- The responsibility for the monitoring and safety of the systems rests with their on-roll school.
- HHELC will support the students to use these systems safely as part of the approach to proactive eSafety awareness.

How will the school respond to any incidents of concern?

- All members of staff will be informed about the procedure for reporting eSafety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The eSafety Coordinator and/or the eSafety working party will record all reported incidents and actions taken in the School incident log and other logs in any relevant areas e.g. Bullying or Child protection log.
- Designated Child Protection Coordinator will be informed of any eSafety incidents involving Child Protection concerns, which will then be escalated appropriately.
- HHELC will manage eSafety incidents in accordance with the school behaviour policy where appropriate.
- HHELC will inform parents/carers of any incidents of concern as and when required. In most cases, this will be in person, on the day of the incident.
- After any investigations are completed, the eSafety working party will debrief, identify lessons learnt and implement any changes required and if necessary, contact the Area Children's Safeguarding Team and/or CEOP.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the **Anti-Bullying Policy.**
- All incidents of cyberbullying reported to the school will be recorded in an incident log and other in accordance with other reporting expectations.
- Evidence will be gathered and stored before being deleted.

Sanctions for those involved in cyberbullying may include:

- Making a copy of the material as evidence.
- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete

content.

- Internet access may be suspended at HHELC for the user for a period of time. Other sanctions for students and staff may also be used in accordance to other policies at HHELC
- Parent/carers of students will be informed.
- The Police will be contacted if a criminal offence is suspected.

How will Radicalisation be managed?

Although serious incidents involving radicalisation have not occurred at HHELC to date, it is important for us to be constantly vigilant and remain fully informed about the issues which may affect Students personally together with wider developments in this area as publicised in the media and on-line. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Designated Safeguarding Officers). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and students. The subject of Radicalisation is dealt with in more detail in HHELC Safeguarding Poilicy.

How will Learning Platforms be managed?

A Learning Platform is a collection of tools that provide secure online space for storing data, learning materials and allowing for online collaboration. At HHELC we use a number of digital tools, including Office 365, provided by Microsoft.

- Staff will regularly monitor the usage of the Learning Platform by students and staff in all areas, in particular message and communication tools and publishing facilities. Such communication tools are restricted to HHELC education staff and students only.
- Students/staff will be advised about acceptable conduct and use when using the Learning Platform, in accordance with the **eSafety Guide.**
- Only members of the current students, parent/carers and staff community will have access to the Learning Platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.
- When staff, students etc leave the school their account or rights to specific school areas will be disabled and stored in our digital vault for as long as it is necessary, in accordance with our Data policy.
- Any concerns about content on the Learning Platform may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the Learning Platform for the user may be suspended.
d) The user will need to discuss the issues with the Headteacher before reinstatement.
e) A student's parent/carer may be informed.

- A visitor may be invited onto the Learning Platform by the Head teacher. In this instance there may be an agreed focus or a limited time slot.

- Where a visitor/commissioner is given access to Office 365 an Acceptable Use Agreement will be signed and access to specific data will be provided for a limited period of time.

How will mobile phones and mobile devices be managed?

- The use of home-owned mobile phones, tablets, ipods etc.… and other personal devices by students is restricted at HHELC.
- Home-owned devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity, with consent from a member of staff and authorised by QMC or TEB Head or as required for medical need by students and this will be authorised by the key teacher.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Any images or video created at HHELC on a home-owned device must be deleted from the device before it is taken home.

Students Use of Personal Devices

- We recognise that for many students they are reliant on access to a mobile phone, in addition access to technology and the web can be related to emotional and health issues. Rather than a blanket policy covering all key stages and situations, we expect that appropriate use of mobile phones is encouraged by all staff under the direction of the Headteacher.
- Where use of a mobile device/home own technology affects engagement in learning, appropriate responses should be taken in accordance with the behaviour policy.
- In HHELC, if a students needs to contact his/her parents/carers they will be allowed to use a school phone or the school office will contact the parent/carer for them. Parents/carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Generally staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity, even after the students ceases to be taught at HHELC Education.
- It must be noted that home tutors may have cause to contact parents/carers using their personal mobile phones. There are dangers for staff in using their personal phones to contact pupils or families and therefore this will only be done when authorised by a member of the senior leadership team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose (The Microsoft Surface Pro has the capacity to take photographs and make video recordings).

- Care should be taken when using a mobile phone or device in school time so as not to compromise professional expectations. eg. even in the staff room or staff kitchen , think about who can view or hear the content from a mobile phone, could they be offended by the content? How would your Headteacher react to viewing this content and is your professional integrity negatively impacted?
- If a member of staff breaches this policy then disciplinary action may be taken.

Communication Policy

- All users will be informed that network and Internet use will be monitored.
- An eSafety training programme/scheme of work will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
- It is the responsibility to ensure that eSafety rules/posters/displays or copies of the students Acceptable Use Policy will be posted in all HHELC sites. Education and responsible use of the Internet and technology will be encouraged across the curriculum. Rules will be adapted and presented in a way that is suitable for the age and maturity of the students in each class.

How will the policy be discussed with staff?

- The eSafety Policy will be formally provided to and discussed with all members of staff at induction.
- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- The eSafety working party will highlight useful online tools which staff should use with children in the classroom and at other learning locations. These tools will vary according to the age and ability of the students.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parent's/carer's attention will be drawn to the **Induction guide for eSafety**.
- A partnership approach to eSafety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting eSafety at other attended events e.g. parent evenings.
- Parents/carers will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.

Complaints

Any complaints relating to an eSafety matter should be made in accordance with the HHELC complaints policy.

END