Online Safety Policy

The Children's Hospital School at Great Ormond Street & UCH		
Review Frequency	Annual by HT	*Next review date: April 2020*
Previous Reviews	April 2017	
Full Governing Body Ratification	n/a	*Date: n/a*
Approving Committee	A&C	*Date:May 2019*
Policy Holders (name of staff)	Bianca Costa/Jayne Franklin	
Published on website	Yes	*Date: ongoing*

The Children's Hospital School GOS Hospital for Children NHS Trust,
Great Ormond Street, London WC1N 3JH
Tel +44 (0) 20 7813 8269 Email head@gosh.camden.sch.uk
www.gosh.camden.sch.uk

Headteacher Jayne Franklin BEd Hons (Cantab)

Table of Contents

1. Online Safety: The Issues

1.1 Introduction

Children and young people are growing up in a world dominated by technology that provides them with access to a wide range of information sources and increased opportunities for instant communication and social networking.

Using the Internet can benefit children's education and give them more opportunities to socialise, but it can also present several risks. Children are often unaware that they are as much at risk online as they are in the real world, and parents and staff may not be aware of the actions they can take to protect them.

In the face of these risks, parents and schools may deal with the problem by denying or limiting access to the Internet; however, this may have little effect as children can access the Internet in a range of localities such as libraries, Internet cafes and on mobile phones.

It is The Hospital School's policy that the educational and social benefits of the Internet should be promoted, but that this should be balanced against the need to safeguard children.

This document outlines the School's Policy in terms of managing risk and taking action to help children use the Internet safely and responsibly. Although it is intended that online-safety strategies and polices should reduce the risk to pupils whilst using the internet, this cannot completely rule out the possibility that pupils may access unsuitable material.

The School cannot accept liability for material accessed or any consequences of Internet access, but all reasonable precautions will be taken to ensure a safe online learning environment.

1.2 Benefits and Risks

Use of technology is so universal that it is of huge benefit to children to learn these skills in order to prepare themselves for the working environment; it is important that staff are aware that the inherent risks are not used to reduce children's use of technology.

1.2.1 Benefits

Technology can make a huge contribution to children's education and social development by:

- raising educational attainment by providing engaging and motivating learning opportunities
- improving research and writing skills
- allowing those with SEND to access the curriculum and overcome communications barriers
- enabling those who are unable to attend school to be taught "remotely"
- improving wellbeing through the social and communications opportunities offered
- providing access to a wide range of differentiated teaching and learning resources and materials.

1.2.2 Risks

The risks associated with use of ICT by children can be grouped into 4 categories.

Content

The Internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and which is not suitable for children. There is a danger that children may be exposed to and damaged by inappropriate images and content, such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

Contact

Chat rooms and other social networking sites can pose a real risk to children as users can pretend to be someone else and take on an alias, or adopt an avatar to represent themselves rather than using their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

Commerce

Children are vulnerable to unregulated commercial activity on the Internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents.

They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent and realising the danger. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people.

- using information from the Internet in a way that breaches copyright laws.

- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience and that material once published on the web is very difficult to remove.

- online bullying (see section 4.1.4 for further details).

- using mobile devices to take and distribute inappropriate images of themselves or peers (youth produced sexual imagery). These cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

- Children may also be adversely affected by obsessive use of the Internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

2. Roles and Responsibilities

2.1 The Role of the Headteacher

The Headteacher has ultimate responsibility for online safety issues within the Hospital School including:

- the overall development and implementation of the school's online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community
- linking with the governing body and parents and carers to promote online safety and implement the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

2.2 The Role of Governors

The governing body has a statutory responsibility for pupil safety. Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors are subject to the same online safety rules as staff members and must sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. Governors must always use their school email addresses when conducting school business.

2.3 The Role of the Online Safety Coordinator

The designated Online Safety coordinator, (Bianca Costa), is responsible for co-ordinating online safety policies on behalf of the School.

They have the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's online safety policy
- ensure that staff and pupils are aware that any online safety incident should be reported to them
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for school staff, governors, pupils and parents
- liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raise the profile of online safety awareness within the school by ensuring access to training and relevant online safety literature
- ensure that all staff and governors have read and signed the acceptable use policy (AUP)

- ensure that pupils have signed the acceptable use policy (AUP) where necessary (see section 3.5)
- maintain a log of internet related incidents and co-ordinate any investigation into breaches
- report all incidents and issues to Camden's online safety officer.

2.4 The Role of the Network Manager

The network manager has responsibility for:

- The maintenance and monitoring of access to the Internet, including anti-virus and filtering systems.
- Carrying out regular monitoring; capturing of evidence (on site and remotely) and audits of networks and reporting breaches to the Online Safety Officer.
- Supporting any subsequent investigation into breaches and preserving any evidence.

2.5 The Role of ALL School Staff

All school staff must ensure that they adhere to the school's online safety policy and procedures. All school staff are also responsible for:

- communicating the school's online safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- reporting breaches of internet use to the online safety co-ordinator
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety officer
- teaching the online safety and digital literacy elements of the new curriculum.

2.6 The Role of the Designated Safeguarding Leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter will be referred to a Designated Safeguarding Lead who will decide, in consultation with the Senior Safeguarding Lead (Headteacher), whether or not a referral should be made to The Trusts' Social Work Departments to be dealt with in accordance with the Hospital Trusts' Child Protection Policies.

3. Online Safety Strategy

3.1 Definition and Purpose

Online safety forms part of the "staying safe" element of the Government's Every Child Matters agenda, and all schools have a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils. Schools also owe a duty of care to children and their parents to provide a safe learning environment.

The School's online safety strategy aims to ensures a safe online learning environment in order to maximise the educational benefits of technology whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

3.2 The System

- The School uses the London Grid for Learning (LGfL) platform which provides filtering software to block access to unsuitable sites.
- All School owned systems have up to date anti-virus software installed and can be monitored remotely by the School's network manager.

3.3 Accessing and Monitoring the System

- Access to School computers is via individual user log-in and password.
- The Network Manager keeps a record of all log-ins used within the School for the purposes of monitoring and auditing Internet use and activity.
- Network and technical staff responsible for monitoring systems are supervised by Online Safety Officer
- Staff carefully consider the location and position of computers in classrooms, on the ward and in other teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

3.4 Confidentiality and data protection

- All data held on the Schools IT systems is held in accordance with the principles of the Data Protection Act 2018. Data is held securely and password protected with access given only to staff members on a "need to know" basis.
- Staff and pupil data that is being sent to other organisations must be encrypted or sent via the secure file transfer site Egress. Any breaches of data security must be reported to the head teacher immediately.

3.5 Acceptable Use Policies

- All staff and Governors must sign an acceptable use policy on appointment (AUP).
- All pupils who attend the schoolroom and work independently on their own school work using the school's equipment must sign the acceptable use policy (AUP).

3.6 Teaching Online Safety

Teaching staff are responsible for delivering ongoing online safety education in the classroom as part of the curriculum.

- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teaching staff may wish to use PSHE lessons as a forum for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.

- Pupils should be taught the elements of online safety included in the computing curriculum so that they:

    - use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

    - can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems

    - are responsible, competent, confident and creative users of information and communication technology.

3.7 Pupils with Special Needs and Disabilities

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the Internet and will require additional guidance on online safety practice as well as closer supervision.

All staff are responsible for providing extra support for these pupils and should:

- Where necessary, liaise with the Online Safety officer and the School's IT team to discuss any requirements for further safeguards to the school's IT system or tailored resources and materials in order to meet the needs of pupils with SEND.

- Ensure that the School's Online Safety Policy is adapted to suit the needs of pupils with SEND.

- Liaise with parents and carers in developing online safety practices for pupils with SEND.

- Keep up to date with any developments regarding emerging technologies and ~~e-~~online safety and how these may impact on pupils with SEND.

3.8 Staff training and conduct

3.8.1 Training

- All school staff and governors receive training with regard to IT systems and online safety as part of their induction.

- Staff also attend annual training on online safety so that they are aware of the risks and actions to take to keep pupils safe online. School management ensure that staff have regular updates in order to ensure they can keep up with new developments in technology and any emerging safety issues.

3.8.2 Conduct

All School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own Internet use, particularly in relation to their communications with pupils.

The following points must be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photos and video images of pupils are only to be taken by staff in connection with educational purposes e.g. School magazine/website.

- Staff must only use School equipment to take images and must only store images on School computer systems.

- Staff must take care regarding the content of, and access to, their own social networking sites and ensure that pupils and parents cannot gain access to these.

- Staff must ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

- Staff must be particularly careful regarding any comments to do with the school that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff must not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute.

- Staff must not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with pupils regarding school work, this should be via their school e-mail account. All emails must be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When contacting parents or pupils by telephone, staff must only use School equipment. Pupil or parent numbers must not be stored on a staff member's personal mobile phone and staff must not lend their mobile phones to pupils.

- When contacting parents or pupils by email, staff should always use their school email address or account. Personal email addresses and accounts must never be used.

- Staff must ensure that personal data relating to pupils is always stored securely and encrypted if taken off School premises. No pupil identifiable data should ever be taken off site (e.g. first name, last name combinations, address and telephone numbers etc.)

- Where staff are using mobile equipment such as laptops provided by the School, they must ensure that the equipment is kept safe and secure at all times and a user name and password combination is required to gain access.

- Staff should be aware that use of LGFL and NHS e-mail is for the purposes of education or School business only, and emails may be monitored.

3.8.3 Exit strategy

When staff leave, they must return any school equipment to the network manager who will ensure that the devices are reset and that the staff member no longer has access to the school's IT system.

3.9 Safe use of technology

3.9.1 Internet and Search Engines

- When using the Internet, children must receive the appropriate level of supervision for their age and understanding. Staff should be aware that often, the most computer-literate children are the ones who are most at risk.

- Pupils should not be allowed to aimlessly "surf" the Internet and all use should have a clearly defined educational purpose.

- Despite strong filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, staff must plan the use of Internet resources ahead of lessons by always checking the suitability of websites to be used and storing information off-line where possible.

- Where staff require access to blocked websites for educational purposes, this should be discussed and agreed with Online Safety Coordinator, who will liaise with the School's Network Manager for temporary access. Staff should notify the Online Safety Coordinator and Network Manager once access is no longer needed to ensure the site is blocked again after use.

- Staff should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively,

appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.9.2 Safe use of applications

School email systems should be hosted by an email system that allows content to be filtered and allow pupils to send emails to others within the school or to approved email addresses externally.

Social networking sites such as Facebook, Instagram and Twitter allow users, over 13, to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas on-line. These can have an educational value.

Chat rooms are internet sites where users can join in "conversations" on-line; **instant messaging** allows instant communications between two people on-line. In most cases, pupils will use these at home although school internet systems do host these applications.

Gaming-based sites allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently, these sites are not accessible via school's internet platform.

Safety rules

- Access to and use of personal email accounts, public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system only allowed for educational purposes and under supervision. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.

- Staff have LGFL and NHS email accounts and must use these for all school related communication. Staff must ensure that they use the appropriate account when sending emails. NHS accounts must be used for all communication within the hospital i.e. to other NHS accounts. LGFL accounts must be used for all other work related emails.

- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.

- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.

- Pupils should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's safeguarding policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.

- Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.

- In order to teach pupils to stay safe online outside of school, they should be advised:

    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
    - to only use moderated chat rooms that require registration and are specifically for their age group;
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.9.3 Video Conferencing

Video conferencing enables users to communicate face-to-face via the Internet using web cameras.

- Video conferencing should only be carried out using approved Google Meet, Facetime or Skype using the school accounts only.
- Pupil use of video conferencing on school owned equipment must be for educational or psychosocial purposes and must be supervised by school staff.

- Pupils must always be appropriately dressed during any photography or filming.

- School owned photographic or video devices may be used by teachers but only in connection with educational activities.

- Photographs and videos should only be downloaded onto secure (user name and password controlled) school owned hardware and should never be associated with individual pupil's full names or other identifying information.

3.9.4 School Website

- Content should not be uploaded onto the School website unless it has been authorised by the Headteacher or Assistant Heads) who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- The School's SLT are responsible for ensuring the content of the School's websites is appropriate.

- To ensure the privacy and security of staff and pupils, the contact details on the website must be The School address, email and telephone number. No contact details for staff (including staff email addresses) or pupils should be contained on the website.

- Pupils' full names should never be published on the website.

- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the School and the intended audience.

3.9.5 Photographic and Video Images

- Where the School uses photographs and videos of pupils online for publicity purposes, for example on the School website, images should be carefully selected so that individual, named, pupils cannot be identified.

- Where photographs or videos of identifiable children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.

- Pupils' full names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the School's computer system and all other copies deleted.

- Stored images should not be labelled with the child's full name.

3.9.6 Pupils' Own Mobile Phone and Handheld Systems

Use of mobile phones and handheld systems is not allowed during lessons / in school unless permission is given by school staff.

Under no circumstances are children allowed to use their phones for taking photos of other children.

Pupils are not able to access the school's internet on their personal devices.

4. Responding to incidents

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety co-ordinator in the first instance. All incidents, whether involving pupils or staff, must be recorded by the online safety co-ordinator on the online safety incident report form (appendix 3).

- A copy of the incident record should be emailed to Camden's designated online safety officer at jenni.spencer@camden.gov.uk.

- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action and consideration given to contacting the LADO where this is appropriate. Incidents involving the Headteacher should be reported to the LADO and chair of the board of governors.

- The school's online safety co-ordinator should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy.

- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the Designated Safeguarding Lead, who will decide, in consultation with the Senior Safeguarding Lead, as to whether or not to refer the matter to the police and/or Trusts' Safeguarding team and Trust Social Work department in conjunction with the Headteacher.

4.1 Types of Incident

4.1.1 Unintentional Access of Inappropriate Websites

- If a pupil or member of staff accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupil's age, staff should immediately (and calmly) close or minimise the screen.

- Staff should reassure pupils that they have done nothing wrong and discuss the incident with the class/pupil to reinforce the online safety message and to demonstrate the School's "no blame" approach.

- The incident should be reported to the online safety co-ordinator and details of the website address and URL provided.

- The online safety co-ordinator should liaise with the network manager and/or Camden Schools' IT team to ensure that access to the site is blocked and the School's filtering system reviewed to ensure it remains appropriate.

4.1.2 Intentional Access of Inappropriate Websites by a Pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will subject to appropriate sanctions (see section 5).

- The incident should be reported to the online safety co-ordinator and details of the website address and URL recorded.

- The online safety co-ordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.

- The pupil's parents / carers should be notified of the incident and what action will be taken.

4.1.3 Intentional Access of Inappropriate Websites by Staff

- If a member of staff witnesses misuse of technology by a colleague, they should report this to the Headteacher and *online safety co-ordinator* immediately.

- The *online safety co-ordinator* should notify the Network Manager so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the online safety incident report form.

- The *online safety co-ordinator* should arrange with the Network Manager to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the Headteacher should take any necessary disciplinary action against the staff member and report the matter to The School Governing Body, where appropriate.

- If the materials viewed are illegal in nature the Headteacher should report the incident to the Trust/s Security and/or the police and The Chair of the Governing Body and follow their advice, which should also be recorded on the online safety incident report form.

4.1.4 Online Bullying

Definition and Description:

Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Online bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- Rude, abusive or threatening messages via email or text.
- Posting insulting, derogatory or defamatory statements on blogs or social networking sites
- Setting up websites that specifically target the victim.
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, Youth produced sexual imagery /“happy slapping”).

Online bullying can affect pupils and staff members. Often, the Internet, the medium used to perpetrate the bullying, allows the bully to remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Dealing with Incidents

The following covers all incidents of bullying that involve pupils.

- Any incidents of online bullying should be reported to the online safety co-ordinator who will record the incident on the incident report form and ensure that the incident is dealt with in line with the school’s anti-bullying approach. Incidents should be monitored and recorded.

- Where incidents are extreme, for example threats against someone’s life, or continue over a period of time, they will be reported to the police as in these cases, the bullying may be a criminal offence.

- As part of online safety awareness and education, pupils should be told of the “no tolerance” policy for online bullying and encouraged to report any incidents to their teacher.

- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, the service provider should be contacted so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address.

- Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents or their teacher. Bullying should be reported to any chat room moderator so that they can take action.

- Where bullying involves messages on social networking sites or blogs, the School should contact the website provider to request that the comments are removed. In extreme cases, the bully’s access to the site can be blocked.

- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

Online Bullying of Staff

- The Headteacher should be aware that staff may become victims of online bullying by pupils. Because of the duty of care owed to staff, Governors and The Headteacher should ensure that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils and parents/carers.

- The issue of online bullying of staff will be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.

- Incidents of online bullying involving school staff should be recorded and monitored by the online safety co-ordinator in the same manner as incidents involving pupils.

- Staff should follow the advice above on online bullying of pupils and not reply to messages but report the incident to the Headteacher immediately.

- Where the bullying is being carried out by parents the Headteacher should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.

4.1.5 Youth Produces Sexual Imagery (Sexting) and sexual abuse / harassment by peers

- The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases, these actions may be harmful or abusive or may constitute harassment or online bullying.

- “Sexting” or the sending of sexual images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

- Staff need to be able to react to incidents in a proportionate manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

- Schools need to be aware of the use of technology by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this.

4.1.6 Risk from Inappropriate Contacts

Staff may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the Internet. The pupil may report inappropriate contacts or staff may suspect that the pupil is being groomed or has arranged to meet with someone they have met online.

- All concerns around inappropriate contacts should be reported to the *online safety co-ordinator* and the Designated Safeguarding Lead.

- The Designated Safeguarding Lead should discuss the matter with the referring member of staff and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to the Trust Social Work Team and or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- The Designated Safeguarding Lead can seek advice on possible courses of action from Camden's online safety officer in Children's Safeguarding and Social Work.

- School staff should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact is possible.

- The designated safeguarding lead and the online safety co-ordinator should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them to discuss what action they can take to ensure their child's safety.

- Where inappropriate contacts have taken place using school equipment or networks, the online safety co-ordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.1.7 Risk from Contact with Violent Extremist

Many extremist groups who advocate violence use the Internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

The School has a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff need to be aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

- The school should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.

- All incidents should be dealt with as a breach of the acceptable use policies. The school's relationships policy and staff disciplinary procedures should be used as appropriate.

- The online safety co-ordinator and the designated safeguarding lead should record and review all incidents in order to establish whether there a particular extremist group is targeting the school and whether current school procedures are robust enough to deal with the issue.

  Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should first refer the young person to the MASH team using an e-CAF in the same way as for other safeguarding referrals.

4.1.8 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor

- Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

5. Sanctions for misuse of School ICT

5.1 Sanctions for Pupils

5.1.1 Category A Infringements:

These are low-level breaches of acceptable use agreements such as:

- Use of non-educational sites during lessons.
- Unauthorised use of MSN Messenger chat type facilities.
- Unauthorised use of prohibited sites or accessing social networking sites during lessons.

School Policy:

Pupils and staff are expected to abide by the School's Acceptable Use Policy (AUP) at all times and use resources responsibly and safely.

5.1.2 Category B Infringements

These are persistent breaches of acceptable use agreements following warnings, or use of banned sites and/or serious breaches of e-safety policy such as:

- Continued use of non-educational sites during lessons continued unauthorised use of email.
- Continued use of prohibited sites for instant messaging or social networking.
- Use of illegal file sharing software.
- Accidentally corrupting or destroying other people's data without notifying staff.
- Accidentally accessing offensive material without notifying staff.

Sanctions could include:

- referral to online safety officer and an oral warning.
- loss of Internet access for a period of time removal of computer until the end of the day.
- contacting parents.

5.1.3 Category C Infringements

These are deliberate actions that either negatively affect the Internet and/or the LGfL or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- Deliberately bypassing security or access.
- Deliberately corrupting or destroying other people's data or violating other's privacy online bullying.
- Deliberately accessing, sending or distributing offensive or pornographic material.

- Purchasing or ordering items over the Internet.
- Transmission of commercial or advertising material.

Sanctions could include:

- Referral to Headteacher and a written warning.
- Loss of access to the Internet for a period of time.
- Reporting to parents.

5.1.4 Category D Infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- Persistent and/or extreme online bullying.
- Deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act.
- Bringing the School's name into disrepute.

Sanctions could include:

- referral to Headteacher and a final written warning.
- Contact with parents.
- Possible exclusion.
- Referral to Hospitals' Social Care Teams (GOS & UCH).
- Referral to community police officer.
- If appropriate, referral to Camden's online-safety officer.

5.2 Sanctions for Staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

5.2.1 Category A Infringements

These are minor breaches of the School's Acceptable Use Policy (AUP) which amount to misconduct and will be dealt with internally by the Headteacher.

- Excessive use of Internet for personal activities not connected to professional development (e.g. social networking, blogging etc).

- Use of personal data storage media (e.g. removable memory sticks without encryption, password protection or carrying out virus checks).

- Any behaviour on the world wide web that compromises the staff member's professional standing in the School and community, for example inappropriate comments about the School, staff or pupils or inappropriate material published on social networking sites.

- Sharing or disclosing School passwords or personal logins to others breaching copyright or licencing by installing unlicensed software.

Possible sanctions include referral to the Headteacher who may issue a warning according to the School's Disciplinary Policy.

5.2.2 Category B Infringements

These infringements involve deliberate or seriously careless actions that undermine safety on the Internet and LGfL and activities that call into question the person's suitability to work with children.

They represent gross misconduct that would require a strong response and referral to Headteacher, School Governors and/or other agencies. For example:

- Repeated Category A infringements (see above).

- Serious misuse of or deliberate damage to any School computer hardware or software, for example deleting files, downloading unsuitable applications.

- Any deliberate attempt to breach data protection or computer security rules, for example hacking.

- Deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.

- Receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act.

- Bringing the School's name into disrepute.

Possible sanctions include:

- Removal of equipment

- Referral to Camden's online-safety officer

- Referral to the police

- Suspension pending investigation
- Disciplinary action in line with the School's Disciplinary Policy

6. Appendix 1

INTERNET ACCEPTABLE USE POLICY FOR PUPILS

I understand that I can use the Internet as long as I behave in responsible way that keeps me and others safe. I also understand that School's network and Internet connection is monitored and that if I do not follow the rules I may not be allowed to use the Internet.

I will:

- not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family or my friends unless my teacher has given permission.
- never arrange to meet someone I have only met on-line unless my parent, carer or teacher has given me permission and I will take a responsible adult with me.
- tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like.
- not use any Internet system to send anonymous or bullying messages to anyone.

PARENTS, CARERS AND GUARDIANS

As the parent or legal guardian of the above pupil, I give permission for my child to use the School's network and access the Internet, e-mail, MSN (or similar chat type facility). I understand that they will be provided with guidance and rules for safe and responsible use of the Internet.

I accept that the School/Hospital cannot be held responsible for the nature and content of materials accessed through the Internet, but I understand that the School/Hospital will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate content. These steps include using filtered/restricted access to the Internet, ad-hoc monitoring of web use during School hours, employing appropriate teaching practice and teaching e-safety to pupils.

I understand that the School can check my child's computer files, and any Internet sites visited, and that if such a check is made and there are any concerns about e-safety or behaviour, they will contact me.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my child's e-safety.

Any inappropriate use of the Internet/network will result in the service being withdrawn and possible disciplinary action, if appropriate.

THE FOLLOWING ARE NOT PERMITTED ON THE SCHOOL NETWORK

- Sending or displaying offensive messages, pictures or web pages.
- Searching for or visiting undesirable or inappropriate web sites or materials.
- Using racist, sexist, homophobic, violent or abusive language during the conduct of e-mails or other Internet activities.
- Using another person's password or divulging your password to others.
- Trespassing in another pupil's work area or files.
- Intentionally wasting limited resources.
- Violating copyright laws.

Declaration:

I have read the rules that apply to using the Internet and I understand that if I break any of these rules I will lose my access to the use of the facilities and further action may need to be taken.

I understand the School will have to report anything inappropriate that is found on my computer (e.g. content of a sexual or abusive nature) to the relevant authorities.

I agree that it is my responsibility, as a parent/guardian/carer to supervise my child's appropriate use of the Internet.	
Pupil's name:	
Parent/Guardian's name:	**Date:**
Parent/Guardian's signature:	

Signature:

Name of supervising teacher:	**Date:**

All data on this form is confidential and is processed in compliance with the "Data Protection Act 2018

7. Appendix 2

Acceptable Use Policy for Staff and Other Employees of The Hospital or Trust(s) Who Require Access to The School's Network & Internet

Access and professional use

- During School hours all computer networks and systems are made available to staff for educational, professional and administrative purposes only.

- Staff are expected to abide by the School's e-safety rules and the terms of this Online Safety Policy. Failure to do so may result in disciplinary action being taken.

- The School reserves the right to monitor Internet and network use and activity and examine and delete files and folders from the School's system.

- Staff have a responsibility to safeguard pupils in their use of the Internet and report all e-safety concerns to the online safety officer.

- Copyright and intellectual property rights in relation to materials used from the Internet must be respected.

- E-mails and other written communications must be carefully written and polite in tone and nature.

- During School hours, staff should only access work related Internet sites via the LGfL; access to personal email accounts, non-work related websites, social networking sites, blogs, Tweets and wikis is not allowed. Failure to comply may result in disciplinary action being taken.

Data Protection and System Security

- Staff must ensure that all confidential data involving pupils sent via the Internet is password protected and encrypted, where necessary. First and last name combinations should not be used to identify a pupil.

- Where data is taken off site, via laptops, iPads, USBs etc., the information must be password protected and encrypted. Any portable media such as USB sticks or CD/DVDs etc. should be virus checked prior to use.

- Downloading unauthorised software is not allowed and all files stored on computers will be regularly checked. Failure to comply may result in disciplinary action being taken.

- Sharing and the use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

- Files stored on the School's network should be archived or deleted if no longer needed.

Personal Use

- Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is immoral or illegal

- Staff should not allow School equipment or systems to be used or accessed by unauthorised persons and should keep any computers used at home safe and secure. Any theft or damage should be reported immediately to the School Business Manager. A police crime number will be required in the event of any theft.

- Staff should ensure that personal websites, social networking websites or blogs do not contain material that compromises their professional standing or brings the School's name into disrepute.

- Use of LGfL/Internet for financial gain, gambling, political purposes or advertising is not permitted.

Declaration:

I have read the above and understand that if I infringe any of these rules I will no longer be permitted to access or use School IT facilities and further action (including disciplinary and/or criminal proceedings) may need to be taken.

Staff Name:
Signed:
Date:

8. Appendix 3

E-safety Incident Report form

This form should be kept on file and a copy emailed to Camden's e-safety officer at jenni.spencer@camden.gov.uk (ONLY if the incident involved a Camden child or young person).

School details:

Name of school:	The Children's Hospital School at Great Ormond Street and University College Hospital
Address:	Great Ormond Street Hospital, Great Ormond Street, London, WC1N 3JH
Name of online safety officer:	Bianca Costa
Contact details:	Telephone: 0207 813 8269
Email:	b.costa@gosh.camden.sch.uk

Details of incident:

Date happened:	**Time:**	
Name of person reporting incident:		
If not reported, how was the incident identified?		
Where did the incident occur?		
* In school/service setting	* Outside school/service setting	
Who was involved in the incident?		
* child/young person	* staff member	* other (please specify
Type of incident:		
* bullying or harassment (cyber bullying)		
* deliberately bypassing security or access		
* hacking or virus propagation		
* racist, sexist, homophobic religious hate material		
* terrorist material		
* drug/bomb making material		
* child abuse images		
* on-line gambling		
* soft core pornographic material		
* illegal hard core pornographic material		
* other (please specify)		

Description of incident:

Nature of incident:

Deliberate access Did the incident involve material being;			
* created	* viewed	* printed	
* shown to others	* transmitted to others	* distributed	
Could the incident be considered as;			
* harassment	* grooming	* cyber bullying	* breach of AUP
Accidental access Did the incident involve material being;			
* created	* viewed	* printed	
* shown to others	* transmitted to others	* distributed	

Action taken:

Staff
* incident reported to Headteacher / Online Safety Officer / Social Care Team (tick)
* advice sought from Safeguarding and Social Care Team
* referral made to Safeguarding and Social Care Team
* incident reported to police
* incident reported to Internet Watch Foundation
* incident reported to IT
* disciplinary action to be taken
* e-safety policy to be reviewed/amended
Please detail any specific action taken (i.e.: removal of equipment);
Child/Young Person
* incident reported to Headteacher / Online Safety Officer / Social Care Team (tick)
* advice sought from Safeguarding and / or Social Care
* referral made to Safeguarding and Social Care Team
* incident reported to police
* incident reported to social networking site
* incident reported to IT
* child's parents informed
* disciplinary action to be taken
* child/young person debriefed
* Online Safety policy to be reviewed/amended

Outcome of incident/investigation

THE CHILDREN'S HOSPITAL SCHOOL

at Great Ormond Street and UCH