Online Safety Policy

Aim

It is the duty of the school to ensure that every child in its care is safe, and the same principles that apply to the school's physical world apply to its 'virtual' or digital world.

This policy document is drawn up to protect all parties including: the students; the staff and all members of the school community who have access to and are users of the schools IT systems, both in and out of the school. It aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements with respect to the use of IT-based technologies.

IT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to give our young people the skills to access life-long learning and employment.

This policy is to be read in conjunction with the: Safeguarding Policy; Behaviour Policy; Safeguarding Children code conduct for staff; Code of conduct for staff; whistle blowing and Disciplinary policies;.

Roles and Responsibilities – Whole School

Online Safety is recognised as an essential aspect of strategic leadership in Evelina Hospital School and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Head ensures that the Policy is implemented and compliance with the Policy monitored.

The designated **Online Safety Co-ordinator** is Anne Hamilton
The designated **Person for Safeguarding** is Kate Bennett.

The Online Safety Co-ordinator ensures the school community keep up to date with e-Safety issues and guidance through liaison with the Local Authority Safeguarding Coordinator and through organisations such as The Child Exploitation and Online Protection (CEOP) and UK Safer Internet Centre. The school's Online Safety Co-ordinator ensures the: Head; senior management; governors and families are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school and should be updated at least annually on policy developments.
The designated **Governor for Child Protection** is Ellena Valizadeh.
The designated **Governor for ICT** is Chaminda Stanislaus.

Roles and Responsibilities - Staff

All staff should have signed, and be familiar with, the Staff Acceptable Use Policy (see appendix) and be aware that this applies to all school IT equipment, whether it is used at school or at home.

Teachers should include e-Safety in the curriculum and ensure that pupils are educated about safe and responsible use, as appropriate. The 'How to use the Internet Safely While in Hospital' guidelines (see appendix) should be on display in classroom areas and pupils should be taught how to minimise online risks and how to report a problem.

Staff should ensure that any pupil who is using a school computer unsupervised has signed the 'Pupil Internet Agreement' Form (see appendix). In the case of pupils under the age of 16, this must also be signed by the pupil's parents.

When accessing the internet, all pupils will see a webpage outlining the ways that they are allowed to use the internet. It is the responsibility of staff to ensure that this information is understood and that pupils are aware that any concerns must be reported to a member of staff.

Everybody in our school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. If staff have children's records on their laptops or on memory sticks it is their responsibility to ensure that they are password protected.

If there is an e-safety incident, staff should follow the 'What we do if...' guidance (see below).

Roles and Responsibilities – Pupils and Parents

Pupils using the internet unsupervised must sign and adhere to the 'Pupil Internet Agreement' Form. In the case of pupils under the age of 16, this must also be signed by the pupil's parents.
Pupils should report any e-Safety concerns to a member of staff. Pupil and parent concerns regarding e-Safety are regularly monitored and used to inform our policy.

Parents are the keystone to our school's success in implementing our Online Safety Policy. They provide the consistency in ensuring that the messages we give about online safety continue to be followed at home. The school's Online Safety Co-ordinator ensures they are kept updated and are able to access training.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites

- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- online bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- extremism
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2016 KCSIE p62-3)

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the: staff member; student's; parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be placed on silent and are only to be used in relation to medical needs. They should be stored out of sight on arrival at school.
- All visitors are requested to keep their phones on silent and not use them in the school rooms or the area of the Atrium used by school during teaching sessions.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including pornography, violence or bullying. Staff mobiles or hand held devices might be searched if there is a level of concern.
- . Staff may use their phones out of teaching sessions, away from any pupils. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Parents wishing to make phone calls during lessons are asked to leave the classrooms.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/Online Safety Co-ordinator and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered. (LGfL schools report to: www.support.lgfl.net)

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the Head Teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all IT equipment by the schools IT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action. (contact Personnel/Human Resources)
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Remove the PC to a secure place and document what you have done.
   - Contact the local police and follow their advice.
   - Contact the Local Authority Designated Officer

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-Safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform CEOP and the LA e-Safety Officer if necessary.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.police.uk/contact_us/
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-Safety Officer.

The school may wish to consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with the designated Person for Safeguarding in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.police.uk/
4. Consider the involvement police and social services.
5. Inform LA e-Safety Officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Head and the Online Safety Co-ordinator. The Online Safety Incident Reporting Form must be filled out for all the incidences mentioned and returned to the Head or the Online Safety Co-ordinator.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology, they must be able to do this without fear.

Information and Support

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

https://www.thinkuknow.co.uk/

https://www.disrespectnobody.co.uk/

https://www.internetmatters.org/

http://saferinternet.org.uk/

http://www.childnet.com/resources/cyberbullying-guidance-for-schools

http://educateagainsthate.com/

https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Appendix

How To Use The Internet Safely While In Hospital
A Guide For Children, Young People, and Parents, Guardians and Carers

1. Why has this guidance been written? To:

- Help protect you and other children and young people from any harm
- Make sure everyone using the Internet understands what is acceptable and what is not allowed
- Encourage children and young people to use the Internet and email safely. It is good to keep in touch with the outside world, friends and family, but you must follow a few important rules.

2. Why do I have to sign an Internet Agreement Form?

- The staff in the school and the Hospital want to help you understand what you can and cannot do. When you sign the form that means you have said you understand and that you will stick to the rules. This means we can allow you to use the internet unsupervised.

3. What can I do?

- You can use the school's connection to the web to visit websites that will help you with your school work and revision.
- You can Google for information that is suitable for your age
- You can access your home school email and learning platform so that you can stay in touch your school and keep up with your school work.

4. What must I NOT do?

- You must not access or try to look at any Internet sites that may put you or other children and young people at risk. That means, just for example, that you must not go to any sites that may show material of a sexual or violent nature that are not suitable for your age.

5. How does the school know what I am doing

- The school has special equipment so that the Network Manger can see exactly what you are doing at any time, even though they are not sitting next to you. It is a bit like a hidden camera. The Network Manager can even interrupt or stop you using your computer, even though they are not sitting next to you.

6. Can I use my own computer on the school network?

- No

7. What can happen if inappropriate material or bad stuff is found?

- This may mean that the School will not let you use their Internet connection or the computer affected. This is so that everyone can be sure that you are not at risk in any way and that you do not put others at risk. You may instead be offered a school laptop and time for the Internet during school teaching time instead, so you will still be able to learn, have fun and stay in touch with friends.

Laptop Loans and Internet Use Agreement

EHS laptops are loaned to young people on the ward only following a risk assessment and needs analysis by a member of school staff. The risk assessment will include a consideration of

1. The pupil's ability to use equipment safely and without causing damage
2. The parent/carer's availability to ensure the laptop is kept save and used appropriately.

Internet access is restricted by the school to ensure appropriate use and safeguard children from inappropriate websites. A discussion needs to be had with the parents/carers and the young person about the reasons for the loan. Where internet access is being requested, explanations need to be given about the restricted access to avoid disappointment.
The Internet Use Agreement below must be discussed and signed by the young person and parent/carer.

Loans will be most successful if a child or young person wishes to: work with a particular piece of preloaded school software; school programmes; the child's home school Managed Learning Network/website and recommended education websites. Parents/carers and/or children may not load their own games/software onto school laptops.
Parents/Carers must complete this form, agree to supervise and return the said laptop to the schoolroom or a ward nurse prior to discharge. Wherever possible, laptops should never be left unsupervised. Laptops should be used with the power adaptor, to ensure the battery remains charged for the next user.

☐ I agree to immediately inform hospital or school staff if an inappropriate website is accidentally accessed.

☐ I agree that my child will only use the computer/Internet for agreed purposes.

☐ I understand that it is my responsibility to supervise my child when s/he is using the computer, to ensure the computer is used with care and kept sage.

Signed _____ (young person)

Signed _____ (parent)

Signed _____ (teacher)

Date _____

Staff Acceptable Use Policy

The purpose of this document is to briefly outline the conditions of Internet and network use.

When you use the Internet it is essential that you take responsibility for your actions in accessing all networked services. All users of the School's network and Internet will be expected to abide by the rules of its use.

The School's Network and Connection to the London Grid for Learning must not be used for any of the following:

1- the creation or distribution of any images, sounds, messages or other material which are obscene, harassing, racist, homophobic, inflammatory, malicious, fraudulent or libellous.
2- publication of material to which you do not have rights and entitlement.
3- any activity that may be considered unethical, immoral or illegal.
4- sending email messages which may interfere with the work of others, or result in the person receiving them losing their work, data or systems.
5- interfering with the functioning of the network in the school, the services providers network, or any other network that can be accessed through the Internet. The user must not attempt to gain unauthorised access to any computer systems, network, data or resources.
6- any use of the Internet that would bring the name of The School or the Local Authority into disrepute.
7- The user must respect the acceptable use policies of any network that they access.

Declaration

I have read the above and I understand if I infringe any of these rules I will lose access to and use of facilities and further action (including criminal proceedings) may need to be taken.

Name: (in block letters) _____ Date: _____

Staff signature: _____

Consent Form for using images

At the Evelina Hospital School, we'd like seek your consent for some of the ways we take and use your photo.

Using your photo helps us to show members of the school community who works here.

We would like your consent in order to take and use your photo in the ways described below. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below, sign and return this form to school.

▪ Use of personal data	▪ Tick (√)
I am happy for the school to use my photo in **displays in school**.	
I am happy for the school to use my photo on the **school website**.	
I am happy for the school to use my photo in the **school newsletter**.	
I am happy for the school to use my photo in **social media**.	
I am happy for the school to share my photo for **use in the media**	
I am happy for the school to **film me teaching**.	
I am **NOT** happy for the school to use my personal data for any of the above purposes.	

If you change your mind at any time, you can let us know by emailing office@evelina.southwark.sch.uk, or telling the school office you wish to remove your consent.

If you have any other questions, please get in touch.

Why are we asking for your consent again?

You may be aware that there are new data protection rules coming in from 25 May. To ensure we are meeting the new requirements, we need to re-seek your consent for some of the ways we use information about you.

We would appreciate you taking the time to give consent again, as we really value being able to use the information in the ways listed above.

Name: _____

Signature: _____ Date: _____

Online Safety Incident Reporting Form

Date/time of Incident:	
Child and/or Workstation/Device name:	
Incident or concern raised:	
What actions were taken, by whom and why?	
Other information:	
Has any computer or hardware been secured? If so, how/where?	
Has the information been recorded and secured? If so, how/where?	
Member of staff reporting concern:	**Signed:**
Online Safety Coordinator/Designated Safeguarding Lead:	**Signed:**
Action taken by Online Safety Coordinator/Designated Safeguarding Lead:	