Children's Hospital School

Online Safety Policy

Date of Approval:	09/06/2026
Approved by:	Executive Headteacher
Date of next review:	June 2028
Signed:	Stephen Readman

Online Safety and Cyber-Bullying Policy

Policy Rationale

The internet is an essential element in 21st-century life for education, business, and social interaction. We have a duty to provide our learners with internet access as part of their learning experience. At The Children's Hospital School we must ensure the safeguarding of all students.

Policy aims

1. To provide all staff with the necessary information and understanding of their roles and responsibilities with respect to online safety.

2. To ensure consistency of good practice.

Online Safety Policy

The Children's Hospital School recognises that ICT, Apps/ online platforms, the internet and Artificial Intelligence (AI), are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the internet, but it also covers mobile phones and other electronic communication technologies and devices. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings as well as fraud, gambling or other harmful activities. This also including sexual harassment and online sexual abuse. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility of the Designated Safeguarding Lead.

1. **Communicating school policy**

This policy is available on the school website for parents, staff, and students to access when and as they wish. Rules relating to the school code of conduct when online, and online safety guidelines can be found in the ICT Acceptable Use Policy and guidance for students given through computing. Online safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed as well as in computing including but not limited to systems and information security, web browsing and concepts for online protection.

2. **Making use of ICT and the internet in school**

The internet is used in school to raise educational standards, to promote pupil/student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education, and business.

We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet for education are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums, and libraries.
- Contact with school and schools in other countries resulting in cultural exchanges between students all over the world.
- Access to subject experts, role models, inspirational people, and organisations. The internet can provide a great opportunity for pupils/students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

For parents:

Children and young people use technology in amazing ways and achieve amazing things as technology opens up new possibilities of learning and gathering information. With the power of the internet, children can create their own websites, music, videos, and images and upload and share them online with friends, family or the whole world. Thanks to mobile phones, laptops and handheld devices such as portable music players and games consoles, they can access the internet from any location, at any time.

Understanding the risks

Advice to parents

- Learning about the benefits and risks of using the internet and other mobile technologies by attending workshops and written communication sent to parents in the form of leaflets and newsletters.
- Discussing online safety concerns with their children.
- Showing an interest in how their children are using technology.
- Encouraging their children to behave safely and responsibly when using technology.
- Modeling safe and responsible behaviours in their own use of technology.
- Using computer programmes to block sinister sites and exercising age-related control methods.

Useful Websites for Parents can be found at
https://www.childrenshospitalschool.leicester.sch.uk/parents/online safety

Learning to evaluate internet content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will face appropriate sanctions.
- If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of Students. If staff or students discover unsuitable sites then the URL will be reported to the school to the Head Teacher, through capturing inappropriate hits. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

3. Managing information systems

The Children's Hospital School use the following software for Filtering and Monitoring which is reviewed monthly by the Safeguarding Team.

Filtering
(Currently Ekte 2025/2026 but moving to Senso)

Monitoring

Alerts generated by Securus the monitoring system sends screen captures of to the Executive Headteacher which are shared with the Designated Safeguarding Lead and Heads of School to address.

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed termly by the Head Teacher and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- making sure that unapproved software is not downloaded to any school computers
- alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced

4. Emails

The school uses email internally for staff and students and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools and organisations for educational purposes.

Staff and students should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes.

This is important for confidentiality. The school has the right to monitor emails and their contents.

- Students should constantly be told not to share passwords

4.1 School email accounts and appropriate use

Staff should be aware of the following when using email for school:

- Staff should only use official school-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school and will be taught to follow these guidelines through the computing curriculum and in any instance where email is being used within the curriculum or in class;

- in school, students should only use school-approved email accounts
- excessive social emailing will be restricted
- students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves
- Students must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
- Students will be educated through the computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

5. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office and Safeguarding Team only.

5.1 Policy and guidance on safe use of students photographs and work

Colour photographs and students' work bring our school to life, showcase our students' talents, and adds interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 2018 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- how and when the photographs will be used
- school policy on the storage and deletion of photographs

Using photographs of individual students

The vast majority of people who take or view photographs or videos of students do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse students through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school's website cannot be reused or manipulated. Only images created by or for the school will be used in public and students may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children;

- Parental consent must be obtained. Consent will cover the use of images in:
    - all school publications
    - on the school website
    - in newspapers as allowed by the school
    - in videos made by the school or in class for school projects

- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the pupil/student.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed.
- For public documents, full names will not be published alongside images of the child. Groups may be referred to collectively by year group.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only. (This is to be discouraged by the school).
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, the photographer will wear identification at all times, and will not have unsupervised access to the pupils/students.

For more information on safeguarding in school please refer to our school **Child Protection and Safeguarding Policy.**

5.2 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the school's **Child Protection and Safeguarding Policy** and **Behaviour Policy.**

5.3 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. **Students are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply to both students and staff.**

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the computing curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of

taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school social media accounts created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils/students to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

6. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyber-bullying they can be used to access inappropriate internet material
- they can be a distraction to learning
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues

The school takes the following measures to ensure that mobile phones are not used in school. Some of these are outlined below:

- school will not tolerate cyber-bullying against either students or staff. Sending inappropriate, harmful or abusive messages is forbidden and anyone who is found to have sent a message of such content will be sanctioned. Mobile phones can be confiscated by a member of staff in line with the Physical intervention, searching, screen and confiscation policy, should a student not follow the steps below.
- Mobile phones must be handed in on arrival or locked away in lockers provided during school hours or any other formal school activities.
- This will improve social interactions, prevent distractions in learning and images or files being sent between mobile phones in school.
- The school will not take any responsibility for personal devices that have been lost, stolen, or damaged.

6.1 Mobile phone or personal device misuse

Students

Students who breach the school policy relating to the use of personal devices will have sanctions put in place in line with the school's behaviour policy.

- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal devices to contact students either in or out of school time.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

7. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school and will consider any educational benefits that they might have. The school keeps up to date with new technologies and is prepared to develop appropriate strategies for dealing with new technological developments quickly.

8. Protecting personal data

The Children's Hospital School believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management, we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the General Data Protection Regulation 2018 and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

ONLINE SAFETY AT HOME

Several sites offer helpful advice to parents, especially with regard to how they can best monitor their child's use of the computer at home. Important and useful information can be found on our school website as well as on the following site: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
We will provide annual updates and support session for parents/carers about online safety for their children.

NATIONAL BODIES

Further support and guidance may be obtained from the following:

- http://www.anti-bullyingalliance.org.uk Information for Teachers and other Professionals who work with Young People.
- www.bullying.co.uk
- The following information can be downloaded from the above website: Safe to Learn: *Embedding anti-bullying work in schools* (2007): Cyber-bullying Guidance and Resources. Safe to Learn Cyber-bullying Summary Leaflet.
- www.ceop.gov.uk