# E-SAFETY POLICY

| | |
|---|---|
| **Prepared By** | Jai Solanki – Head of IT |
| **Approved By** | Trust Board – July 2020 |
| **Policy Review Date** | July 2023 |

| | |
|---|---|
| **Reviewed By** | Nell Giles - Headteacher |
| **Adopted By** | School Governing Body – May 2021 |
| **Policy Review Date** | October 2022 |

# E-SAFETY POLICY

The school recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at Southampton Hospital School want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning exciting and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security

To enable this to happened we have taken a whole school approach to E-safety as promoted by British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the school's ICT infrastructure and technologies.

The school as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.

The School is committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

The nominated senior person for the implementation of the school's E-safety policy is Nell Giles (Headteacher).

## SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E-safety behaviour that take place out of school.

## ROLES AND RESPONSIBILITIES

The following section outlines the E-safety roles and responsibilities of individuals and groups within the school:
In a small school some of the roles described below may be combined, though it is important to ensure that there is sufficient "separation of responsibility" should this be the case.

### Governors:

Governors are responsible for the approval of the E-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about E-safety incidents and monitoring reports. A member of the governing body has taken on the role of E-safety governor (it is suggested that the role may be combined with that of the child protection/safeguarding governor). The role of the E-Safety governor will include:

- regular meetings with the E-afety co-ordinator/officer
- regular monitoring of E-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant governors/board/committee

### School leaders:

- School leaders have a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the E-safety co-ordinator/officer.
- The school leader and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff

- The school leaders are responsible for ensuring that the E-Safety coordinator/officer and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The senior leadership team will receive regular monitoring reports from the E-safety co-ordinator/officer.

## E-Safety coordinator/officer:

- leads the E-safety committee
- takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
- provides training and advice for staff
- liaises with the Trust
- liaises with school technical staff
- receives reports of E-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-safety governor/director to discuss current issues, review incident logs and filtering
- attends relevant meeting of governors
- reports regularly to senior leadership team

## Network manager/technical Staff:

(NOTE: If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the E-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school's E-safety policy and procedures.)

The Network manager/technical staff/co-ordinator for ICT/computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required E-safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- that the use of the network/internet/virtual learning environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the senior leader/E-Safety coordinator/officer for investigation/action/sanction
- that monitoring software and systems are implemented and updated as agreed in school policies

## Teaching and support staff

are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the Staff acceptable use policy/agreement (AUP)
- they report any suspected misuse or problem to the senior leader/E-safety coordinator/officer for investigation/action/sanction
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Child Protection/Safeguarding Designated Person/Officer should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate on-line contact with adults/strangers
    - potential or actual incidents of grooming
    - cyber-bullying
    - use of school devices outside of the school network (Laptops/Tablets taken home for work), should be used in safe environments, and any sensitive data kept secure.

## Students:

- are responsible for using the school digital technology systems in accordance with the Student acceptable use policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety policy covers their actions out of school, if related to their membership of the school

## Parents/carers

- Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local E-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at school events
    - access to parents' sections of the website/VLE and on-line student records
    - their children's personal devices in the school / school (where this is allowed)

## Community users

Community users who access school systems/website/VLE as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

# POLICIES AND PROCEDURES

The school understands that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist with the school are aimed at providing a balance between exploring the educational potential of new technologies and providing safeguards to pupils.

## Use of internet facilities, mobile and digital technologies

The school will seek to ensure that internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

The school expects all staff and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:
Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive to peers or colleagues.

The school recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

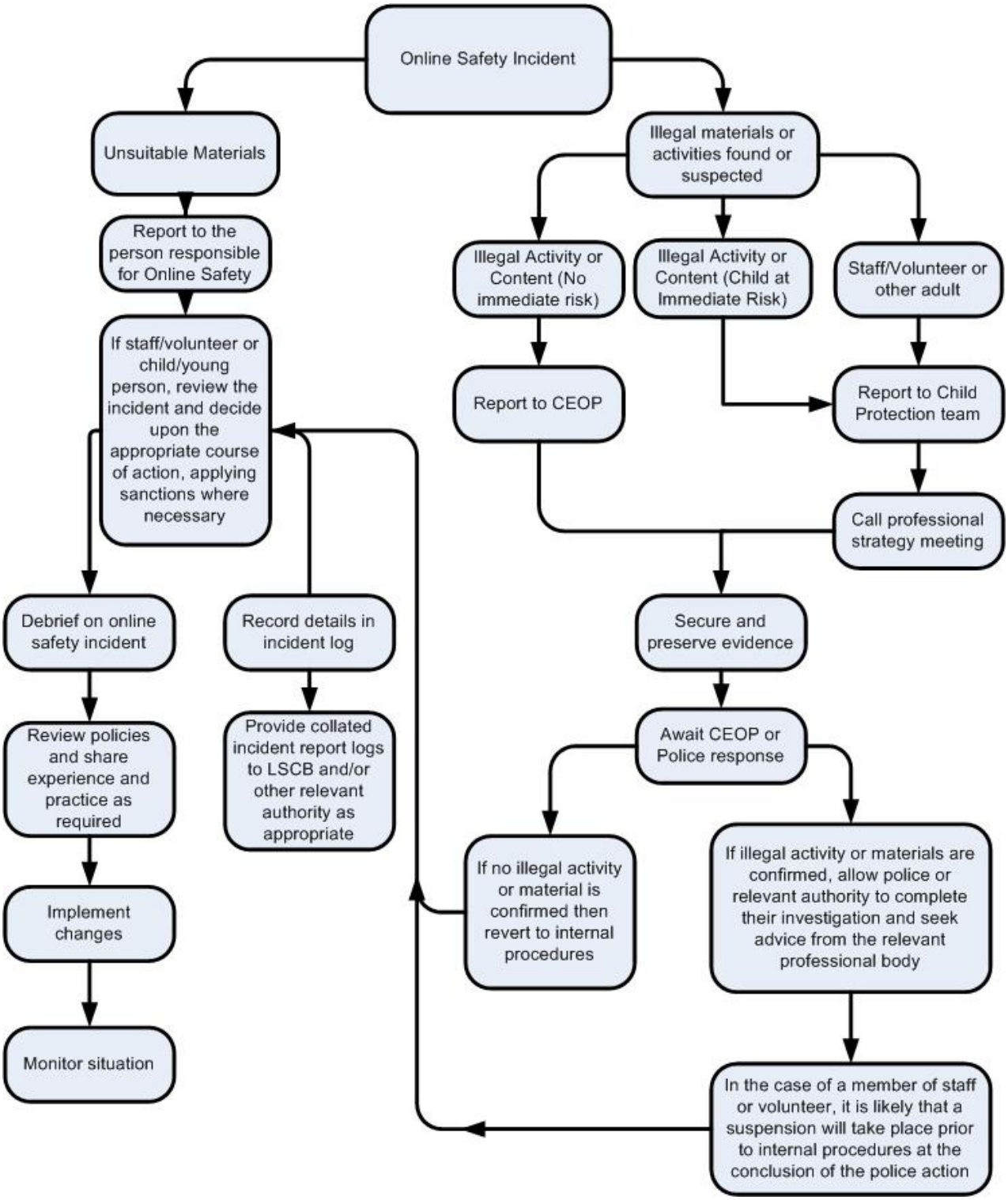
- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity
- Use the school's broadband for running a private business;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the internet
- Use the internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe
- Undertake activities with any of the following characteristics:
  - corrupting or destroying other users' data
  - violating the privacy of other users

- disrupting the work of other users
- using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
- Other misuse of the network, such as introduction of viruses

- Use mobile technologies or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal

# REPORTING ABUSE

The following outlines what to do if a child or adult receives an abusive email or accidentally accesses a website that contains abusive material.




**CEOP – Child Exploitation and Online Protection**

**LSCB – Local Safeguarding Children Board**

## SANCTIONS

The school has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

Where there is inappropriate or illegal use of the internet and digital technologies, the following sanctions will be applied:

- Student
  - The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of internet and email being withdrawn
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns

- Staff and volunteers
  - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
  - Serious breaches may lead to the incident being reported to the police or other regulatory bodies, for instance, illegal internet use or child protection concerns.

## DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

This E-safety policy has been developed by a working group made up of:

- Headteacher and senior leaders
- Staff – including teachers, support Staff, technical staff
- Governors
- Community users – including NHS colleagues
- Members of the Hamwic Education Trust

Consultation with the whole school community has taken place through a range of formal and informal meetings.

**Schedule for development/monitoring/review**

The school will monitor the impact of the policy using**:**

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
- students
- parents/carers
- staff