THE COTTESLOE SCHOOL
E-SAFETY POLICY – NOVEMBER 2018

Reviewed at Resources and People Committee: 21 November 2018
Adopted at Full Governing Body meeting: 12 December 2018
Review date: Autumn Term 2021

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The School's E-Safety Policy will operate in conjunction with other policies including those for:

- Behaviour Management
- Anti-Bullying
- Child Protection
- Computer Resources for Students and Staff
- Privacy Notice

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of the e-Safety Policy in both administration and curriculum, including secure School network design and use.

- Safe and secure broadband service including the effective management of web filtering.

The Cottesloe School acknowledges the assistance of BucksGfl in providing content in this document.

November 2018

1. Naturally policy must be translated into practice to protect students and educate them in responsible ICT use.

1.1 Implementing and reviewing the E-Safety Policy

- The E-Safety Policy relates to other policies including those for ICT, Anti-bullying and Child Protection.

- The Cottesloe School has an E-Safety coordinator who is the Designated Safeguarding Lead as the roles overlap.

- Our E-Safety Policy has been written by the School, building on Bucks County Council E-Safety Policy and government guidance. It has been agreed by senior management and approved by Governors.

- The E-Safety Policy and its implementation will be reviewed every three years.

- The E-Safety Policy was revised by Chloe Hankin (Designated Safeguarding Lead).

1.2 What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones, tablets and smart watches;
- Internet communications: e-mail and IM;
- Webcams and videoconferencing;
- Wireless or wired games consoles.
-

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing ‘incitement’ sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

If there is a suggestion that a student is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection and safeguarding procedures.

2. Teaching and learning

2.1 Why internet use is important

- The purpose of internet use in School is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School’s Management information and administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- It is an essential element in 21st century life for education, business and social interaction.

- Access to the internet is an entitlement for students who show a responsible and mature approach to its use. Our School has a duty to provide students with quality internet access
- Students will use the internet both in and outside of School and will need to learn how to evaluate internet information and to take care of their own safety and security.

2.2 How Internet use benefit education?

Benefits of using the internet in education include:

- access to learning wherever and whenever convenient;
- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between students world-wide;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational; materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Bucks County Council and Department for Education;
- access to learning wherever and whenever convenient.

2.3 Internet use will enhance learning

- The School internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.4 Students will be taught how to evaluate internet content

- The School should ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy e.g. 'fake news'
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- About the risks associated with using the internet and how to protect themselves and their peers from potential risks.
- How to recognise suspicious, bullying or extremist behaviour.
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- The consequences of negative online behaviour.
- How to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the school will deal with those who behave badly.

3. Managing Information Systems

3.1 Information system security

- The security of the School information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Bucks County Council advisors.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.

- Unapproved system utilities and executable files will not be allowed in students work areas or attached to e-mail.
- Files held on the Schools network will be regularly checked.
- The Network Manager will review system capacity regularly.
- Staff memory sticks will need to be encrypted to ensure that school and student data is protected at all times.

3.2 E-mail

The school uses email internally for staff and students and externally for contacting parents and conducting day to day school business and is an essential part of school communication. The school has the right to monitor emails, attachments and their contents but will only do so if there is suspicion of inappropriate use. Staff and students should regularly change passwords and ensure that passwords are effective

Students should be aware of the following when using email in school:

- Students will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class.
- All students are provided with a school gmail account and students may only use approved email accounts on the school system during school hours.
- Students should not use their personal email accounts to contact staff. Staff should not respond to any further emails from the original email account unless the nature of the communication raises safeguarding concerns.
- Students are warned, via the Acceptable Use Agreement not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Students should immediately inform 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.
- Access in School to external personal e-mail accounts will be blocked.
- E-mail sent to an external organisation should be written carefully and staff should adhere to guidance in the professional behaviour policy.
- The forwarding of chain letters, 'jokes' or offensive material is not permitted.

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

- Staff should use their school email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by a member of the Leadership Team.
- Staff must tell a member of the 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.
- Staff should refer to the Data Protection and Confidentiality Policy before sending any sensitive or personal data via email.
- E-mail sent to an external organisation should be written carefully and staff should adhere to guidance in the staff code of conduct.
- The forwarding of chain letters, 'jokes' or offensive material is not permitted

3.3 Published content and the School website

The school website is viewed as a useful tool for communicating the school ethos and practice to the wider community. It is also a valuable resource for prospective parents and students, current parents, students and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting the school. The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered, by the Leadership Team, in terms of safety for the school community, copyrights and transparency policies. The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

- The contact details on the website should be the School address, e-mail and telephone number. Staff or students personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material will be held by the School, or be attributed to the owner where permission to reproduce has been obtained.

3.4 Publishing students' images and work

- Photographs that include students will be selected carefully and any student whose photos are used will need to have parents' permission for these to be published.
- Students' full names will not be used anywhere on the website or on social media, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the School Website.
- Work can only be published with the permission of the student and parents.

3.5 Social networking and personal publishing

The school encourages parents with children under the age of 13 to follow the guidance of social media sites such as Facebook, Snapchat etc. and not give their child access.

- The Cottesloe School will block/filter access to social networking sites. Except for the purpose of the school social media accounts used by selected staff members.
- Students will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or School.
- Teachers' official blogs or wikis should be password protected and run from the School website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- 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 students to remember that they are always representing the school and must act appropriately.
- The Cottesloe School is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Staff that have any social networking sites shouldn't have any links connecting them to The Cottesloe School visible on their page(s)
- School maintained social media accounts will be monitored on a regular basis and can be viewed through the school website.

- Staff are strongly advised not to have any social networking accounts, however those that choose to have one must ensure that their security settings are set to the highest available.

3.6 Managing filtering

- The Cottesloe School will work in partnership with external agencies to ensure systems to protect students are reviewed regularly.
- If staff or students discover an unsuitable site, it must be reported to the E-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the School believes to be illegal must be reported to appropriate agencies such as CEOP (Child Exploitation & Online Protection Centre).
- The Cottesloe School uses E2BN to filter the school users access to the internet.
- The staff have access to appropriate software on the School network which allows monitoring and filtering within individual classrooms.

3.6.1 Contact with violent extremists

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists 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. Bucks LA provides interventions under the Channel project which is part of the Government's Prevent Strategy to divert young people away from extremism.

Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups. The school will ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.

The E-Safety Co-ordinator, along with the Network Manager, should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting young people. If there is evidence that a young person is becoming deeply enmeshed in the extremist narrative, staff will seek advice from Bucks Prevent Officer to prevent radicalisation.

3.7 Managing videoconferencing and audio conferencing

The equipment and network

The school uses school owed laptops for all video and audio conferencing.
Skype is used for all video conferencing calls.

- All videoconferencing equipment in the classroom must be switched off when not in use.
- The equipment must be secure and if necessary locked away when not in use.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the School Website.

Users

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the students' age.
- Parental permission will be sought for children to take part in videoconferences, this includes photographic permissions.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page.

- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing is a challenging activity with a wide range of learning benefits.
- Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that the material being delivered is appropriate for the students.

3.8 Managing mobile and emerging technologies

Mobile phones and other personal devices are now an important part of everyone’s life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- 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

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the school community what is expected of them in terms of respecting their peers, members of the public and staff and any intentional breach of this will result in disciplinary action. Any incidents of cyberbullying will be dealt with in accordance with the Behaviour and Exclusions Policy and, where appropriate, the school's Child Protection and Safeguarding Policy

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.
- Mobile phones will not be used during lessons or formal School time and must be switched off whilst in School.
- The sending of abusive or inappropriate text messages is forbidden as is the videoing or photographing of others without permission.
- Staff will be issued with a School phone where contact with students is required, for example on School trips.
- Wireless network connection is available for both staff and sixth form student owed mobile devices. This is also applicable to laptops owed by staff, sixth form and some SEN students. Access is only available via the Network Manager once a virus check has taken place. Once accessed the user is still bound by the access restrictions as per the School network.
- Students will need to remove any smart watches along with mobile phones whilst sitting any exams, these will be kept in students bags outside of the exam room.
- Staff are not permitted to use their mobile phones whilst in school, with the exception of in the staff room, staff work room or personal offices. However, this is only applicable when there are NO students present.
- Staff are encouraged to not access their school emails on their mobile devices.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

4. Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign (accept) the 'Computer Resources Staff Code of Practice' before using any School ICT resource.
- The School will maintain a current record of all staff and students who are granted access to School ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the Online Safety Acceptable Use Agreement
- Parents will be asked to sign and return an Online Safety Acceptable Use Agreement
- Parents will be informed that students will be provided with supervised internet access.

4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. Neither the School nor Bucks County Council can accept liability for the material accessed, or any consequences resulting from internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the Policy monitored.
- The School should audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.
- Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher, if it is against the Headteacher then the Chair of Governors must be informed.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure which can be found in the Complaints and Resolutions Procedure via the School website.
- Parents and students will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions within the Behaviour Management Attitude to Learning Policy include:
  - interview/talking with the Head of Year;
  - informing parents or carers;
  - removal of Internet or computer access for a period of time.

4.4 Community use of the Internet

- The School will liaise with local organisations to establish a common approach to E-Safety.
- The School will be sensitive to internet related issues experienced by students outside of School, e.g. social networking sites.

5. Communication of the Policy

5.1 Introducing the E-Safety Policy to Students

- E-Safety posters will be displayed in all rooms with computers.
- Students will be informed that network and Internet use will be monitored.
- An E-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An E-Safety module will be included in the PSHCE and ICT programmes covering both School and home use.

5.2 Staff and the E-Safety Policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible internet use and on the School E-Safety Policy will be provided as required.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the School Website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Parents will need to also sign an Online Safety Acceptable Use Agreement

6. E-Safety Contacts and References

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Think U Know website
http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

7. Acknowledgements

This E-Safety guidance is based in part on the publication “Schools E-Safety Policy 2007” by Kent County Council and we gratefully acknowledge their permission to use it in the production of this document.

8. Review

This policy will be reviewed in three years (earlier if any legislative change).

November 2018

Online Safety Acceptable Use Agreement
Secondary Pupils

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Pupils are expected to read and discuss this agreement with you and then to sign below as indicated and to follow the terms of the agreement. Any concerns or explanation can be discussed with Their form tutor in the first instance

Please can you also sign and return the parent/carer agreement below.

This document will be kept on record at the school.

- I will only use school IT equipment for school purposes.
- I will not download or install software on school IT equipment.
- I will only log on to the school network, other school systems and resources using my own school user name and password.
- I will not reveal my passwords to anyone other than a parent/carer.
- I will not use my personal email address or other personal accounts on school IT equipment.
- I will make sure that all my electronic communications are responsible and sensible.
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately, to a member of staff if I am in school or parent/carer if I am not in school.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- I should never post photographs, videos or livestream without the permission of all parties involved.
- I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
- I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.

- I will not attempt to bypass the internet filtering system in school.
- I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
- I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

✂---

Pupil agreement

Pupil name: ……………………………………………………………………………………….

I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature: ……………………………………………………………………………………

Parent/s Carer/s agreement

Parent/s Carer/s name/s: ………………………………………………………………………….

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.)

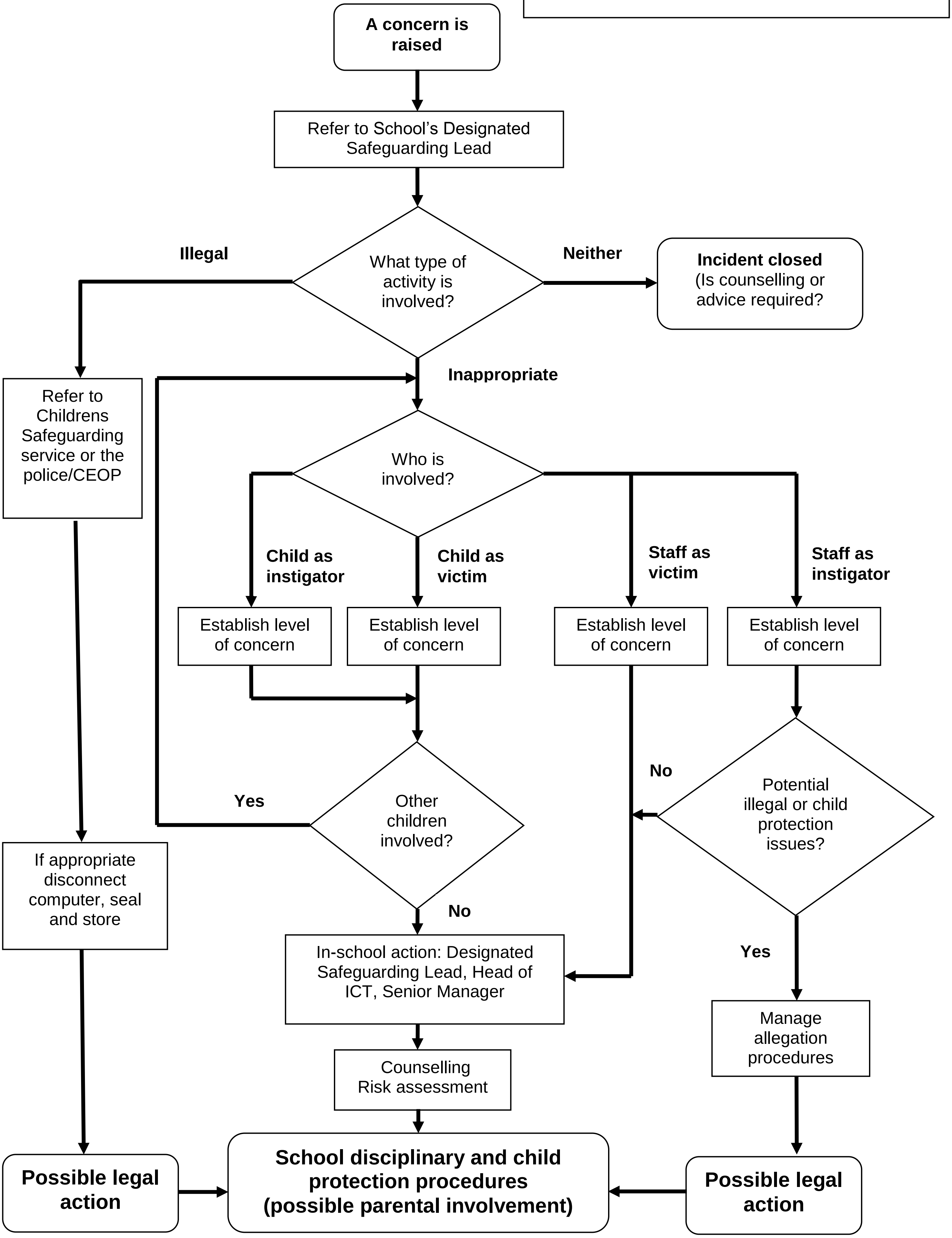
I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent/carer signature: ……………………………………………………………………………

Date: ……………………………………………………………………………………………….

Response to an incident of concern

How do we respond?
The flowchart below illustrates an approach to investigating such an incident.


A concern is raised
Refer to School's Designated Safeguarding Lead
What type of activity is involved?
Illegal
Neither
Incident closed (Is counselling or advice required?
Inappropriate
Refer to Childrens Safeguarding service or the police/CEOP
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern
Establish level of concern
Establish level of concern
Establish level of concern
Other children involved?
Yes
No
No
Potential illegal or child protection issues?
Yes
If appropriate disconnect computer, seal and store
In-school action: Designated Safeguarding Lead, Head of ICT, Senior Manager
Manage allegation procedures
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures (possible parental involvement)
Possible legal action