E-SAFETY POLICY

Reviewed by Governors: September 2024 **Next review:** September 2025

The e -Safety policy will be reviewed annually.

What is e-Safety?
Information and Communications Technology (ICT) is an essential education tool. With its benefits come dangers. Students now work online in school and at home and have personal devices not covered by network protection. Therefore, everyone needs to understand the risks and act accordingly. The key points of this policy are summarised below:

- N Ahmed is the designated e -Safety Coordinator for the school
- Password security is essential for students and staff, particularly for staff as they are able to access and use student data.
    - Staff are expected to have secure passwords which are not shared with anyone.
    - Students are expected to keep their passwords secret and not to share with others, particularly their friends.
- Staff and students are regularly reminded of the need for password security.
- All users read and accept an Acceptable ICT Use Agreement to demonstrate that they have understood the school's e -Safety Policy.
- Staff should not use their own mobile phones to contact parents except in the case of an emergency when they can adjust their phone to ensure that the caller ID is withheld. They must also inform the Headteacher and/or Designated Safeguarding Lead.
- Staff must never take images or make videos of students covertly on any device
- Staff must ensure that any images or videos that are made are created for teaching and learning purposes
- Students must never take images or make videos of students on any device, unless directed by the teacher
- The school allows staff to bring in personal mobile phones and devices for their own use
- The school allows students to bring in personal mobile phones and devices however they are to be handed in at the start of their day.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- All staff should refrain from using mobile phones in lessons and in corridors, except in an absolute emergency or if they are being used for relevant note taking, calendar functionality or the school-provided programme.
- Data stored on a USB stick is, generally, not encrypted. **Do not store sensitive information on a portable device. Advice on how to password protect your USB device can be obtained from the Dataspire team**

Introduction
ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, internet technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies. At Little Ilford School we understand the responsibility to educate our students on e -Safety issues, teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in and beyond the context of the classroom. Both this policy and the Acceptable ICT Use Agreements are inclusive of both fixed and mobile internet technologies provided by the school, such as PC's, laptops, mobile phones, tablet PCs, webcams, whiteboards, voting systems, digital video equipment, digital cameras, visualisers, etc. and technologies owned by students and staff brought onto school premises, such as laptops, ipads, mobile phones and smartwatches etc.

Roles and Responsibilities
As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Ms N Ahmed has been designated the role of e -Safety coordinator within the school. All members of the school community have been made aware of who holds this post. It is the role of the e -Safety coordinator to keep abreast of current issues and guidance through organisations such as London Borough of Newham, CEOP (Child Exploitation and Online Protection) and Childnet..

Senior Leaders and Governors are updated by Ms N Ahmed (e -Safety coordinator) and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's Acceptable ICT Use Policy for staff, governors, visitors and students, is to protect the interests and safety of the whole school community.

Teaching and learning

- The purpose of Internet use in Little Ilford School is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Students use the internet widely outside the school and will need to learn how to evaluate internet information and to take care of their own safety and security.

The Internet enhancing learning

- Students will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- 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.
- Students will be taught to ensure that they have a saved copy of the latest version of every piece of coursework on which they are working on the school network.

Evaluating Internet content

- If staff or students discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the Network Manager.
- The school should ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Managing Internet Access

- The security of the school ICT systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with Dataspire
- The Network Manager will review system capacity regularly.

Managing email

- The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or student based, within school or international.

At Little Ilford School, the school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged. Email histories can be traced if necessary.
- School business should only be conducted from school email accounts.
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal email addresses.

- Email sent to an external organisation should be written carefully before sending, in the same way as one would draft a letter written on school headed paper.
- Students may only use school approved accounts on the school system - Google classroom and/or littleiilford.org email to contact teachers or staff
- Students must tell a teacher/trusted adult immediately if they receive an offensive email.
- Staff must inform the e -Safety Coordinator/line manager if they receive an offensive email.
- All information shared with the Governing Board will be through GovernorHub.

Safe Use of Images and Film

- Digital images are easy to capture, reproduce and publish and therefore could be misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness of the action. With the written consent of parents (on behalf of students), the school permits the appropriate taking of images by staff and students with school equipment under the following guidance:

At Little Ilford School:

- Staff that wish to take photographs or videos with their students as a keepsake may do so in certain circumstances:
    - It should be declared to a senior member of staff prior to the event
    - The images / videos should never be taken covertly and always with the full consent of the students and their parents;
    - It should not be shared online or any social media account;
    - It should always be appropriate and not used to undermine or embarrass a student.

Parents

- Will not be allowed to film and take images of their child during performances and will be reminded at the beginning of any performance that no image or video may be taken. The school will endeavour to provide parents with a school video/photographs to buy as keepsakes of their child's performance at minimal cost.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students or staff within the school environment, or when on educational visits, unless pre-approved by a member of staff.

Publishing students' images and work

- On a child's entry to the school, all parents / carers will be asked to give permission to use their child's work/photos in the following ways:
    - On the school website.
    - On the school's Learning Platform.
    - In the school prospectus and other printed publications that the school may produce for promotional purposes.
    - In display material that may be used in the school's communal areas.
    - In display material that may be used in external areas (i.e. exhibitions promoting the school).
    - General media appearances (e.g. local/national press to highlight an activity, sent using traditional methods or electronically).
- This consent form is considered valid for the entire period that the child attends this school unless:
    - There is a change in the child's circumstances where consent could be an issue (e.g. divorce of parents, custody issues etc.). Parents/carers may withdraw permission in writing at any time.
- A potential risk of publishing students' images and work on the internet/ social media is that a child may become of interest to a sex offender. Locating people through the internet has become extremely easy, using widely available software, so if a picture contains the name of

a school, setting or youth group and the full name of the child or adult then it could be quite easy to find out someone's exact location or address which could then put them at risk.

Therefore, we at Little Ilford School follow the procedure of never publishing a child's full name alongside their photograph.

Storage of Images at Little Ilford School:

- Images/films of children are stored on the school's network and are not to be used by the teacher on any personal or social media platform.
- Students and staff are not permitted to use personal portable media for storage of images without the express permission of the Head Teacher.
- Rights of access to this material are restricted to staff and students within the confines of the school network.

Data Security

- The accessing and appropriate use of school data is something that the school takes very seriously in order to comply with the Data Protection Act 1998.

At Little Ilford School:

- Staff are aware of their responsibilities when accessing school data. Level of access is determined by the Headteacher and implemented by the Deputy Headteacher for Assessment and the Data Manager.
- Any data taken off the school premises must be encrypted. (Advice must be sought from the Dataspire Technician when doing this).

Copyright

The infringement of copyright is a criminal offence under the Copyright, Designs and Patents Act 1988 and could result in prosecution.

- Just because something is on the web does not mean it is freely available for you to use in your own work. As with any material which is protected by copyright, you should seek the author's permission if you wish to use it. With text you can use up to 5% of any one piece of work without seeking permission. With images, sound, animations, and video clips, you should seek permission, unless you are specifically told you can download and use them freely.
- Copyright law allows students special concessions but these are very limited. As a member of staff or a student you may use copyright material for your own personal study purposes only. This includes using copyright material as part of an assignment. If you later want to use the same material for any other purpose, you must seek permission.
- You should always acknowledge the source of any 'third party' material you include in your own work.

Portable and Removable Storage Devices (RSD)

Over recent years, staff have increasingly needed to be fully mobile and connected, often taking information home or out of the school in order to maintain productivity and deliver services efficiently and effectively.

- Staff should seriously consider whether the use of RSD (e.g. A USB stick), is appropriate. Staff can access student data securely using CC4 Anywhere or through their Google classroom account or by logging onto Go4Schools
- Data stored on a USB stick is, generally, not encrypted. **Do not store sensitive information on a portable device. Advice on how to password protect your USB device can be obtained from the Dataspire Technician.**

Child Protection – (see Appendix 2 Student flow diagram)

- Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to risk of harm. Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.
- It is known that adults who wish to abuse children may pose as children to engage, and then meet up with, the young people with whom they have been in communication. This process is known as 'grooming', whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones. An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.
- Increasingly bullying is conducted on the internet or by the use of text messages/social media applications and is therefore harder for schools to notice and deal with.
- As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress.

If 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 (see appendix 1 Staff flow diagram):

1. Report to and discuss with Ms N Ahmed (e -Safety coordinator and DSL) in school and contact parents.
2. Advise the child on how to terminate the communication and attempt to save all evidence.
3. Contact Child Exploitation and Online Protection centre (CEOP) at www.ceop.gov.uk
4. Consider the involvement of police and social services.
5. Consider informing the Local Authority e -Safety officer.

- Students 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.

Cyberbullying Guidance

- Cyberbullying is bullying through the use of communication technology like mobile phone text messages, emails or websites. This can take many forms for example:
    - Sending threatening or abusive text messages or emails, personally or anonymously.
    - Making insulting comments about someone on a website, social networking site (e.g. Facebook/Snapchat/Instagram) or online diary (blog).
    - Making or sharing derogatory or embarrassing videos of someone via mobile phone or email.
    - Abusive language or images used to bully, harass, threaten another, whether spoken or written (through electronic means) may be libellous and may contravene the Harassment Act 1997 or the Telecommunications Act 1984.

Within our School Behaviour Policy and Acceptable ICT Use Agreement (Section 10), the use of the web, text messages, social media sites, email, video or audio to bully another student or member of staff will not be tolerated.

- Bullying can be conducted verbally, in writing or images, including through communication technology (cyberbullying) e.g. graffiti, text messaging, email or postings on websites. It can be done physically, financially (including damage to property) or through social isolation.

If a bullying incident directed at a student or member of staff occurs using email or mobile phone technology either inside or outside of school time:

- Advise the student/staff member not to respond to the message.
- Refer to relevant policies including E-Safety Policy, Acceptable ICT Use Policy and Anti-bullying policy and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's email service provider.
- Notify parents of the children involved or, in the case of a member of staff, refer to your Line Manager
- Consider informing the police depending on the severity or repetitious nature of offence.
- Consider Informing the Head Teacher and LA E-Safety officer depending on the severity.

If malicious or threatening comments are posted on an Internet site about a student or member of staff:

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Send all the evidence to an appropriate point of contact via the e -Safety incident flowchart.
- Endeavour to trace the origin and inform police as appropriate.
- Consider informing the Head Teacher or LA e -Safety officer.

Misuse and Infringements

- Any misuse of computer equipment or mobile technology that breaches any of the guidelines set out in the e -Safety policy should be reported to the e -Safety coordinator. Should an infringement of the school's Acceptable Use Agreement, e -Safety Policy or Removal Storage Device Policy occur, please report it to Ms N Ahmed, Deputy Headteacher.
- Students found to be in infringement of this policy will be subject to sanctions as outlined the Behaviour Policy. Staff may be subject to disciplinary action.

Inappropriate material

- At Little Ilford School all users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the teacher or Naveen Ahmed, e -Safety Coordinator depending on the seriousness of the offence.
- Serious infringements may result in investigation by the Head Teacher/LA and could lead to immediate suspension, possibly leading to dismissal and involvement of police.

Equal Opportunities

- The school endeavours to create a consistent message with parents and carers for all students and this in turn should aid establishment and future development of the schools' e -Safety policy. However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e -Safety issues.
- Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of e -Safety. Internet activities are planned and well managed for these children and young people.

Password Security

- Password security is essential for students and staff, particularly for staff as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to

share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and accept an Acceptable ICT Use Agreement to demonstrate that they have understood the school's e -Safety Policy.
- Users are provided with an individual network log-in. From Year 7 they are also expected to use a personal password and keep it private.
- Students are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised, or someone else has become aware of your password, report this to the Dataspire
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, data, Go4Schools, Satchel, Maths Watch, and Google classroom learning portfolios, including ensuring that passwords are not shared and are changed periodically. Individual users must also make sure that workstations are not left unattended and are locked.
- Under no circumstances are staff allowed to let any other person use their username and password. ***This could result in disciplinary action*.**

Staff Mobile Devices

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device. If a call does need to be made, the Headteacher and the DSL should be informed beforehand.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Staff must not use mobile phones (texts/calls) in lessons, in corridors or when on duty, except in an absolute emergency. The only exception (whilst in the corridor/on duty) is in order to log behaviour/praise incidents using satchel. SLT may need to use their phone if an incident is taking place..
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile Devices

- The sending of inappropriate text messages between any members of the school community is not allowed.
  Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as mobile phones, laptops and ipads for educational visits, only these devices should be used.

Published Content - Website

- 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.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Photographs that include students will be selected carefully and will not include personal details so individual students will not be clearly identified.
- Students' full names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Website.
- Students' work can only be published with the permission of the student and parents.
- Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated.

Students, Parents and Carers

- All students are advised to be cautious about the information given by others on sites. This is because other people may not be who they claim to be.
- Students, parents and carers are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students, parents and carers are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, school details, email address and specific hobbies/interests).
- Students, parents and carers are advised to set and maintain profiles on such sites to maximise privacy and deny access to unknown individuals.
- Students, parents and carers are asked to report any incidents of bullying to the school.
- Information leaflets are available in Reception.
- The school advises parents and carers to locate PCs and laptops in a highly visible part of the home, which can be regularly monitored.
- Students should not meet anyone that they have met through the internet, unless accompanied by a trusted adult.

Social networking and personal publishing

- Little Ilford School has a Service Level Agreement (SLA) with Dataspire to block/filter access to social networking sites.
- Students are 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, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Students are advised not to place personal photos on any social network space. They should assess how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location (e.g. house number, street name, school, shopping centre).
- Teachers must not run social network spaces for students on a personal basis or to give/accept friendship requests from students on social networking sites.
- The school is aware that bullying (including sexual harassment) 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.
- The school will work in partnership with parents, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If you are a member of a social networking site (e.g. Facebook) ensure that your security settings are high. If you need further advice on this matter, see the Dataspire
- Staff who are members of social networking sites are advised not to accept past (under the age of 18) and current students as friends.
- Staff are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- School laptops/ipads are only to be used by the staff member allocated the laptop/ipad. The laptop/ipad should not be used by family members and should only be used for work purposes and appropriate personal use.
- Under no circumstances should staff take any images and videos taken within the school environment off site without the authorisation of the Headteacher
- Staff must refuse an invitation to link with a colleague on a social networking site until they have checked with the colleague that the request is genuine.

Managing E-Safety within School

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- The school maintains students will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology, e.g. e-Safe.
- Staff will preview any recommended sites and materials before use.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- The school endeavours to deny access to social networking sites to students within school.

Infrastructure

- RM and the London Grid for Learning have a monitoring solution where web-based activity is monitored and recorded. The school makes use of e-Safe software to track and monitor all account activity when staff and students have logged in through RM Unify
- School internet access is controlled through the London Grid for Learning's web filtering service.
- Little Ilford School is aware of its responsibility when monitoring staff communication under current legislation and takes into account the Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998.
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or students discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the class teacher.

Filtering and Monitoring systems

- G*overning bodies and the headteacher do all that they reasonably can to limit children's exposure to the risks from the school's IT system. As part of this process, governing bodies and the headteacher ensure the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.*
- *The Department for Education's filtering and monitoring standards set out that schools should:*
  → identify and assign roles and responsibilities to manage filtering and monitoring systems.
  → review filtering and monitoring provision at least annually.
  → block harmful and inappropriate content without unreasonably impacting teaching and learning.
  → have effective monitoring strategies in place that meet their safeguarding needs.
- *Filters and Safeguards for illegal content cannot be disabled by anyone (including the system administrator)*
- *The school filtering system manages both discriminatory content and content that constitutes hate speech*
- *The school considers the extent to which (http and https) content is analysed as it is streamed in real time to the user and blocked*

Managing E-Safety outside of school

- Web technologies, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Videoconferencing

The equipment and network

- Videoconferencing should be supervised appropriately for the students' age.
- When recording a lesson, written permission is obtained from 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 is to be stored securely.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Dialogue with other conference participants takes place before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

Emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed through the Senior Leadership Team and the Teaching and Learning team.

Personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Internet Access

- The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date; for instance, a member of staff may leave or a student's access be withdrawn.
- Access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Risk Assessment

- 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 international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- 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.

E-safety complaints

- Complaints of internet misuse by students will be referred to the senior member of staff who line manages the relevant year group. The standard punishment will be removal of internet access (apart from ICT lessons) of 2 weeks for KS3 and 1 week for KS4. Parents will be shown the offending material in a meeting arranged at the school.
- Cyberbullying will be dealt with under the Anti-Bullying and Behaviour policies policy.
- Any complaint about staff misuse must be referred to the e -Safety coordinator.

Internet use across the community

- The school will be sensitive to internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.

Communications Policy

- Rules for internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- A module on responsible internet use will be included in the RSHE, Citizenship and ICT programmes covering both school and home use.
- All students read, accept and sign our 'Acceptable Internet Use Policy'.

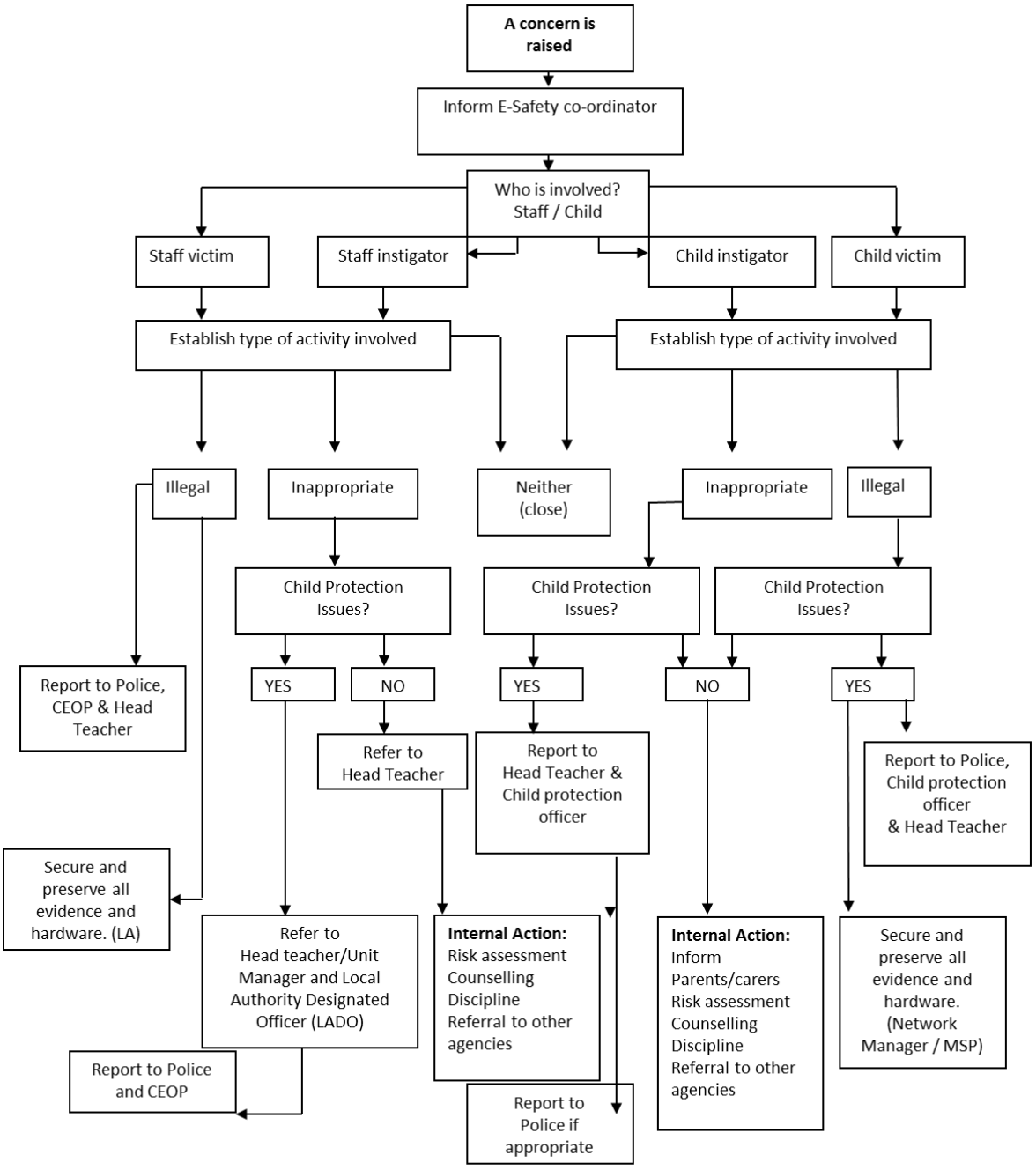
Employees

- All staff must accept the terms of the ‘Acceptable Internet Use Agreement’ statement before using any Internet resource in school.
- 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 development in safe and responsible internet use and on the school e-Safety Policy will be provided as required.
- Staff should not keep photos or videos of students on their personal electronic devices.

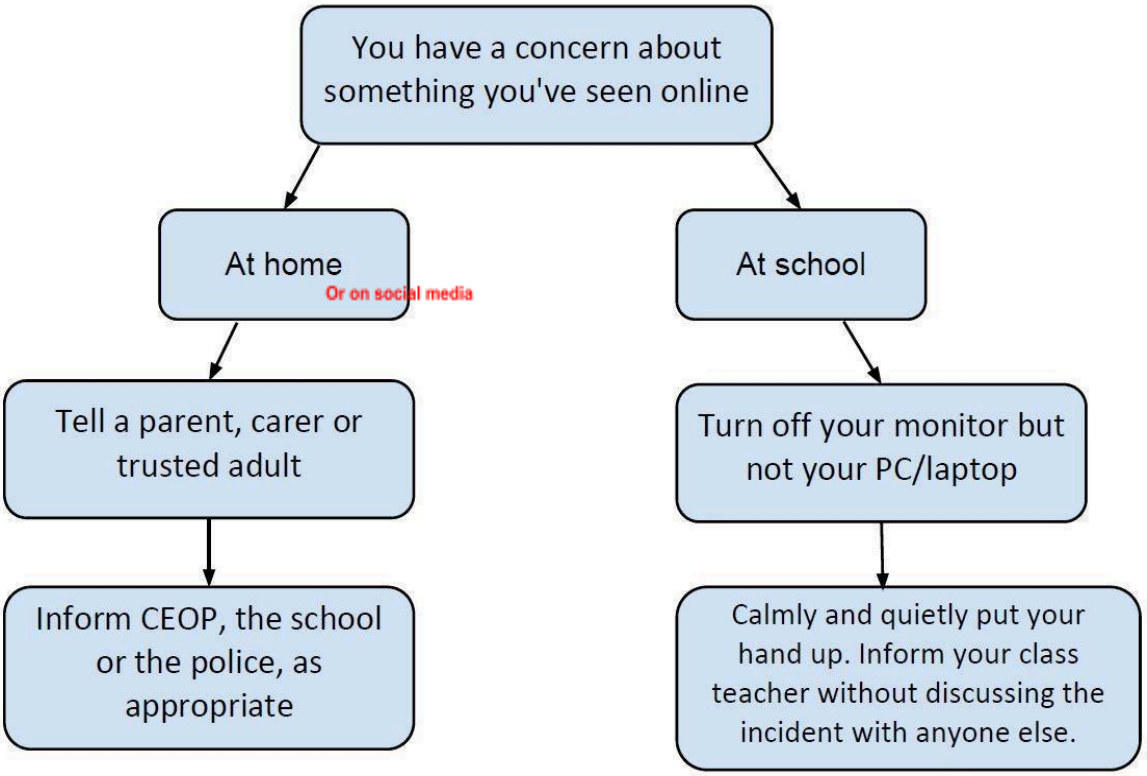
Parental Support

- Parents’ attention will be drawn to the School e - Safety Policy in newsletters and on the school website.

Staff Flow Diagram



Student Flow Diagram



CEOP REPORT
ceop.police.uk

https://ceop.police.uk/CEOP-Reporting/

*If a parent, carer or trusted adult is not available, students are advised to contact the police.