The Winston Churchill School
Online Safety Policy

Review by:	SLT
Adopted by the SLT/Full Governing Body:	November 2022
Next review:	November 2024

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four key categories of risk:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
2. **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
3. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The designated safeguarding governor will meet with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSLs and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Manage online safety issues and incidents inline with the school's child protection policy.
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate levels of security protection procedures such as filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. This is monitored daily.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMs

This list is not intended to be exhaustive.

3.5 All staff

All staff, including agency staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'. Report on CPOMs.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites such as:
- What are the issues? - UK Safer Internet Centre

3.7 Visitors, volunteers, contractors and members of the community

Visitors and members of the community who have a need to use the school's ICT systems or internet will be made aware of this policy, but they will be expected to read, understand and agree to the terms on acceptable use (appendix 1).

4. Educating students about online safety

Students will be taught about online safety as part of the Personal Development Programme including Relationships and sex education and health education curriculum:

This new requirement includes aspects about online safety; these expectations in italics below:

Students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

This is not an exhaustive list.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE) FROG. This policy will also be shared with parents.

Online safety will also be covered during BSBS evenings for parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying: Refer to Antibullying Policy

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies, as well as within the Winston Extra Programme.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL and Headteacher will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. If a search is related to a safeguarding concern staff will follow KCSIE.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police and confiscate the device on instruction from the police, if they are investigating abuse online.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

8. Students using mobile devices in school

Students may bring mobile devices into school but are not permitted to use them during the school day, this includes using a smart watch for the purpose of communication, recording or research.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. Any allegation made about use related to the safeguarding of children will be reported to the LADO.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies, will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

All staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The on line monitoring system, Net Support, is monitored daily and reports made to DSL, Year Leader or Headteacher. The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

The policy will be reviewed annually by the e-safety officer and Headteacher and amendments presented to the governing body for consideration, following a risk assessment of the harms children may face on line.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying Policy
- Staff disciplinary procedures
- GDPR/Data protection policy and privacy notices
- Complaints procedure

The Law

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Computer Misuse Act 1990

This legislation makes it a criminal offence to gain unauthorised access to another students area even if you don't change/delete any information on the area.

Appendix 1

THE WINSTON CHURCHILL SCHOOL

STAFF AND VISITOR

Acceptable Use Agreement / ICT Code of Conduct

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the IT Service Manager.

1. I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
2. I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
3. I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
4. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
5. I understand that I am responsible for all activity carried out under my username, and will not allow any other person to use my login. I will ensure to log out or lock the screen upon leaving my PC/laptop, even if only for a short while.
6. Guests or other staff members may use a computer I have logged in for circumstances such as presentations, but I will remain responsible for my accounts usage and will not leave the guest unsupervised. If guests need to be left unsupervised they should be given a temporary logon and sign the ICT Code Of Conduct document, by request from the HR Manager.
7. I will not enable or permit the access and use of my school staff accounts to students under any circumstances.
8. I will be responsible for monitoring students when supervising them in student ICT rooms and familiarise myself with the schools classroom monitoring software (NetSupport School) and it's appropriate use to safeguard our students.
9. I will ensure that all electronic communications with students and staff are made though the school email system, learning platform, school app or if available a school mobile phone. Any communications must be compatible with my professional role.
10. I will only use the approved, secure email system(s) for any school business.
11. I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
12. I will not install any hardware of software without the permission of IT service manager.
13. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
14. Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Head teacher.
15. I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

16. I will respect copyright and intellectual property rights.
17. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. Online activities include (and are not limited to) social media websites (e.g. Facebook, Twitter, LinkedIn), blogs, video sharing, discussion forums, wiki and other personal webspace.
18. No recommendation will be made by staff for students to use any social networking sites.
19. I understand that social networking sites (e.g. Facebook, Twitter) will not be accessible on the school network. If such sites are required for teaching and learning I will consult the IT Service manager to allow access.
20. I will report any incidents of concern regarding children's safety to the E- Officer, the Designated Safeguarding Lead or Head teacher.
21. I will ensure that electronic communications with students including email, instant messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
22. I will support the school's E-safety policy and help students to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

Additional terms for staff with extended IT rights

1. I will respect colleague's rights to privacy, and will not seek to view or observe their screens or electronic files without a support requirement or request from the school's Headteacher, IT Service Manager or Governing Body.
2. I shall not enhance or alter the system rights assigned to myself by the IT Service Manager.
3. I shall not facilitate external access to the school system to myself or any other person without authorisation from the IT Service Manager.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name……(printed)

Job title……

Signature…… Date……

Appendix 2

Responding to an E-safety incident

This is guidance for senior management within schools, regarding how to respond to an E-safety incident of concern. It is important to note that incidents may involve an adult or child as the victim or the instigator. Adults are also subject to cyber bullying by pupils.

The first section outlines key E-safety risk behaviours. The flowchart on page 18 illustrates the approach to investigating an incident of concern. This diagram should be used with the screening tool (page 19) and the Surrey Child Protection Procedures which include what to do if you are concerned about a child, or about an adult working with children. The School DSL will be conversant with these and the processes for referral. They are available on the SSCB website at: http://www1.surreycc.gov.uk/cafis/manual/index.html

What are the E-safety risks?

The explosion in technology over the last 10 years, in particular the Internet, has provided endless opportunities for children, young people and adults to gain access to information and to communicate with each other. The Internet is an unmanaged, open communications channel, via which anyone can send messages discuss ideas and publish material – and it's these very features which make it an invaluable resource used by millions of children every day. But it is these same features which present a number of risks to children. The vast majority of children's experiences will be positive - but we must be aware that this new technology can be used to bully others, and be manipulated by people who wish to do harm to children.

Risk Behaviours:

Online grooming and child abuse

There are a number of illegal actions that adults can engage in online that put children at risk:

- Swapping child abuse images in chat areas or through instant messenger with other adults or young people and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught
- Swapping personal information of children that they have collected with other abusers
- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex

[Cyber] bullying

In addition to face-to-face bullying, bullying via technology is becoming increasingly prevalent.
"Cyber bullying" is the use of Information and Communications Technology, ICT, particularly mobile phones and the internet, deliberately to upset someone else. "Cyber bullying" is when a child or young person is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child or young person (or group) using the Internet, interactive and digital technologies or mobile phones.

It can be an extension of face to face bullying, with technology providing the bully with another route to harass their target. It differs in several ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity. The 'usual' boundaries of face-to-face bullying are not observed – the bully is not restricted by the size, age or location of their victim.

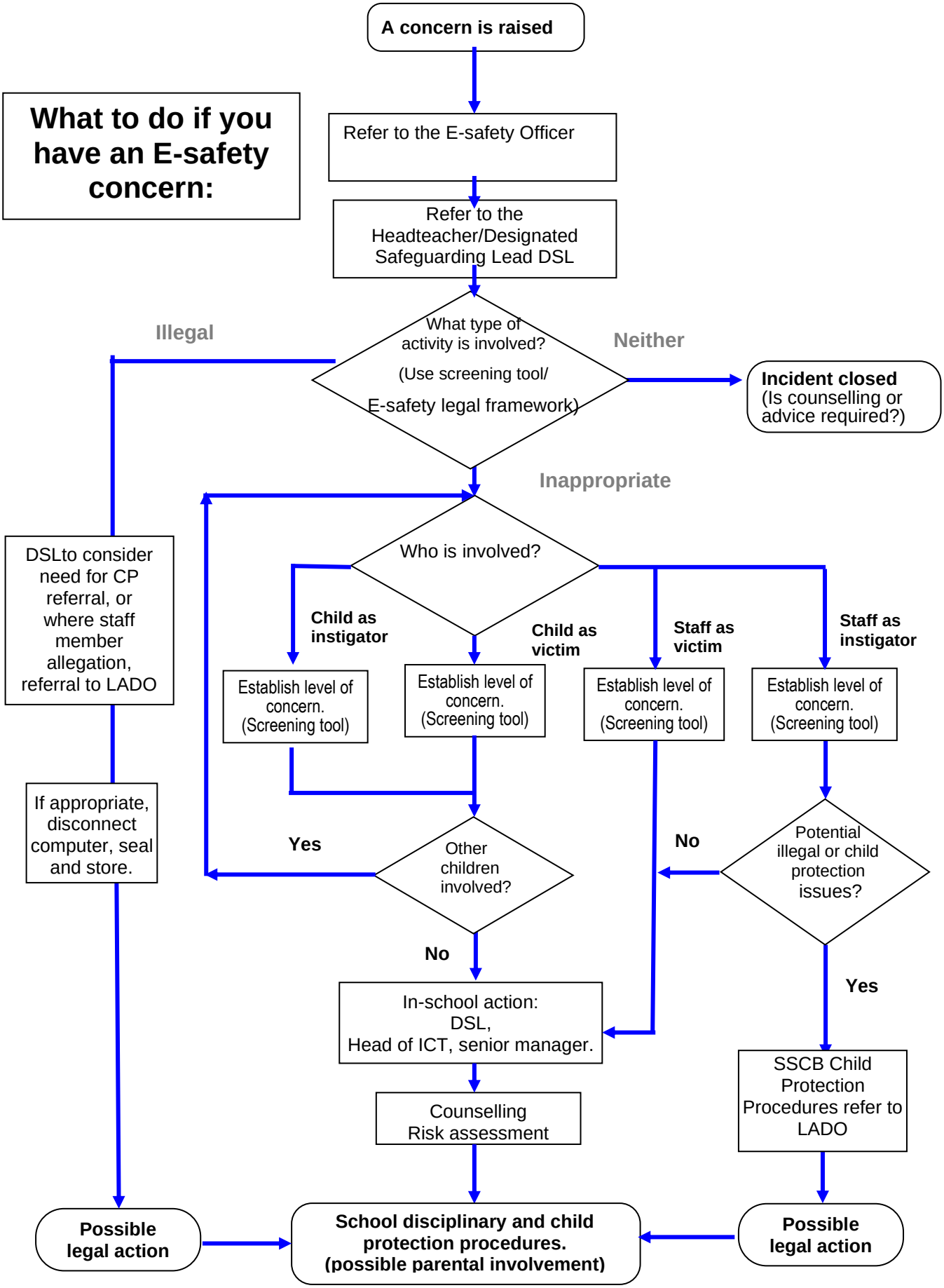
Inappropriate or illegal content

Because it's so easy to upload information onto the Internet, much online content is now inaccurate or extreme – yet is often presented as fact. A great deal of the material on the Internet is published for an adult audience, and some is unsuitable for children. For example, there is information on weapons, crime and racism, access to which would be much more restricted elsewhere.

Disclosing personal information and identity theft

Publishing personal information about themselves online could compromise children's security, and that of those around them. Furthermore, as soon as a message is sent or an image is posted, it can be shared, copied and changed by anyone. Children need to think carefully about their online 'etiquette'.

What to do if you have an E-safety concern:



Duty LADO: 01372 833310 (Local Authority Designated Officer)
Contact Centre Children's referrals 0300 200 1006