The Winston Churchill School

E-SAFETY CODE of CONDUCT and POLICY

Review by:	SLT
Adopted by the SLT/Full Governing Body:	June 2017
Next review:	June 2019

Aims

- To safeguard the welfare of students and staff
- To ensure security and confidentiality
- To safeguard the facilities and uphold the school reputation
- To provide students with a safe high quality ICT experience as an essential part of their learning
- To set out the monitoring and follow up procedures of any e-safety breaches

Objectives

- To provide robust, safe internet access for all students and staff, and identify and manage any associated risks
- To promote and secure the welfare of all students through clear communication of expectation, protocol and procedure for all users of ICT
- To rigorously monitor and review ICT use and practice by all and take appropriate actions to safeguard the school and its users.
- To teach and communicate to students what internet use is acceptable and what is not and give clear expectations for Internet use
- To educate all students in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- To make explicit to students and staff the procedures for reporting inappropriate and offensive Internet and ICT content e.g. using the CEOP Report Abuse icon

General Statement

The Winston Churchill School recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to

enhance skills and enable students to achieve. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the school and to support staff and students to identify and manage risks independently. Monitoring and reporting procedures will be in place to ensure that our e-environment remains safe. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In our duty to safeguard students, we will do all that is reasonable to enable our students and staff stay e-safe and to satisfy our wider duty of care. This E-safety policy should be read in conjunction with other relevant school policies, including Safeguarding Students: Child Protection, the Behaviour Policy, the Anti-bullying policy and the whistleblowing policy.

The policy applies to all students, staff and all members of the school community who have access to the school IT systems, both on the premises and remotely. Any user of the school IT systems must adhere to and sign a hard copy of Acceptable Use Agreement (App 1) and the e-Safety Rules (App 2). The E-safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites, including images, text and sound. This document will set out the school policy with regards to e-safety, but will also give guidance in dealing with any breaches.

Managing Internet Access to ensure security and confidentiality

Information system security

- School ICT systems security will be reviewed yearly and in the event of a breach.
- Security strategies will be discussed with the Local Authority.

E-mail

- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to student email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known and you are expecting an attachment from them.
- The school will consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the website should be the school address, office e-mail and main office telephone number. Staff or student personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual students.
- Students' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of students are published on the school Web site.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate students in their safe use e.g. use of passwords.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any social network space provided in the school learning platform.
- Students and parents will be advised that the use of social network spaces outside school brings a range of dangers.
- Students will be advised to use nicknames and avatars when using social networking sites.
- No recommendation will be made by staff to use any social networking sites.

Managing filtering

- The school will work to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, the site must be reported to the E-safety Officer.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students need to ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones, cameras and other handheld devices will not be used during lessons or formal school time except as part of a staff sanctioned educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff will use a school phone where contact with students is required.
- The appropriate use of Learning Platforms will be discussed as the technology progresses

Protecting personal data

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

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' 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 Responsible Internet Use statement found in their day books.
- Any person not directly employed by the school will be asked to read and sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT to establish its E-safety safeguarding procedures and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of misuse will be dealt with in the first instance by the E-safety Officer.
- Any complaint about staff misuse with regards to e-safety must be referred to the head teacher.
- Students and parents will be informed of consequences for students misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communicating the E-Safety code of conduct to students, staff and parents

Introducing the E-safety policy to students

- Appropriate elements of the E-safety policy will be shared with students
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for students
- All must read and sign the E-safety consent form (App 3)

Staff and the E-safety policy

- 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.
- All must read and sign the ICT code of conduct (App 1)

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /student agreement when they register their child with the school.
- The school will provide support in the form of information and training for parents and guardians.

Roles and Responsibilities

There are clear lines of responsibility for E-safety within the school. The first point of contact for staff should be the E-safety Officer, who will then communicate issues of concern to the e-Safety Safeguarding Officer/ Deputy Headteacher where deemed appropriate to do so.

- All staff are responsible for ensuring the safety of students and should report any concerns immediately to their subject leader and the E-safety Officer.
- Teaching staff are required to deliver E-safety lessons to classes.
- When informed about an E-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.
- All students must know what to do if they have E-safety concerns and who to talk to. In most cases, this will be their teacher, Year Leader or E-safety Officer in the first instance.
- Where any report of an E-safety incident is made, all parties should know what procedure is triggered and how this will be followed up.
- Where the E-safety Officer considers it appropriate with a student at possible serious risk, the Designated Safeguarding Lead (DSL) will be asked to intervene with appropriate additional support from external agencies.
- Appendix 5 provides an e-safety flow chart to guide staff through how to report any e-safety breach.

- Appendix 6 provides guidelines as exemplars in how to deal with various e-safety breaches.

E-Safety Officer: (ESO)

The E-safety Officer is responsible for leading policy review, delivering staff development and training, recording incidents, reporting any developments and incidents to the E-safety Safeguarding Officer and liaising with the local authority and external agencies to promote E-safety within the school community. He/she may also be required to deliver workshops for parents.

E-Safety Safeguarding Officer (ESSO)

The E-Safety Safeguarding Officer, a member of the Senior Leadership Team, will action and sanction students resulting from serious incidents of ICT/internet misuse as reported by, and in liaison with, the E-safety Officer. He/she will also be responsible for communicating with the police, parents, the DSL, the Headteacher and outside agencies as appropriate in addressing such incidents.

Students

Students are responsible for using the school ICT systems and mobile devices in accordance with the school Acceptable Use Policy and the E-safety Rules, which they must agree to and sign. Students are responsible for attending e-safety lessons as part of the curriculum. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an E-safety incident has taken place involving them or another member of the school community. Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

Staff:

All staff are responsible for using the school ICT systems and mobile devices in accordance with the school Acceptable Use Policy and the E-safety Rules, which they must actively promote through embedded good practice. Staff are responsible for attending staff training on E-safety and displaying a model example to students at all times. All digital communications with students must be professional in tone and content at all times. Online communication with students is restricted and must only be done through the school network or the VLE. All staff should apply relevant school policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the E-safety Officer and subject leader without delay.

Governors:

The link governor will hold the school accountable for monitoring and reporting practice in line with the E-Safety policy, reporting to the Full Governing Body (FGB).

<u>Positions of Responsibility</u>

E-Safety Officer - Mrs R Smith

E-Safety Safeguarding Officer / Deputy Headteacher – Mr J Burrows

Designated Safeguarding Lead– Mannan Mohamed

ICT Services Manager – Mr J Coll

Website Administrator – Mrs Ann Cochrane

ICT link governor – tbc

Safeguarding link governor Mr Andrew Erskine

Behaviour

The Winston Churchill School will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy. The school will not tolerate any abuse of ICT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police. This includes incidents of cyberbullying.

Sanctions (see appendix 4)

The school will take all reasonable precautions to ensure E-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Staff and students are given information about infringements in use and sanctions. Sanctions include:

- Interview, counselling and/or disciplinary action by the teacher, Subject Leader Year Leader, E-safety Officer, E-safety Safeguarding Officer or Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to LA / Police
- Internal and external exclusion

Our E-safety Officer will act as first point of contact for any complaint, in the first instance, reporting to the E-safety Safeguarding Officer as deemed appropriate. Any complaint about staff misuse will be referred to the Headteacher and may result in formal disciplinary proceedings. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy with police involvement being the norm.
Complaints related to child protection are dealt with in accordance with school policy Safeguarding Students: Child Protection and LA child protection procedures.

Monitoring, Review and Impact

The impact of the policy will be monitored regularly with a full review being carried out at annually, undertaken by the E-Safety Officer and senior leadership team, Safeguarding Strategic Group, link governor for ICT, staff and students. In the event that any concerns are raised in the interim, triggered by incidents or unforeseen circumstances, the review of policy will be brought forward.

Signed: Chair of Committee…… Date:……

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

The Winston Churchill School

E-safety Rules

These E-safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- I understand the school owns the computer network and learning platform and can set rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes. I will not use ICT systems at school for private purposes, unless the Headteacher has given specific permission.
- I will not use ICT systems at school for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will only log on to the school network/ learning platform with my own user name and password.
- I accept that I am responsible for all activity carried out under my username.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible, particularly as email could be forwarded to unintended readers.
- I will not send anonymous messages or chain mail.
- I will be responsible for my behaviour when using the Internet/learning platform. This includes resources I access and the language I use.
- I will be polite and appreciate that other users might have different views to my own.
- I will use the discussion forums on the school's learning platform for exchanging information and will share my ideas constructively.
- I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using the school's learning platform. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will not deliberately 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 my teacher.
- I will not download or install software on school technologies.
- I will not attempt to bypass the Internet filtering system.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress.
- I will respect the privacy and ownership of others' work on-line at all times.
- I understand the school can exercise its right to monitor the use of the school's computer systems and learning platform, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I understand that all my use of the Internet, school's learning platform and other related technologies can therefore be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted. I understand that irresponsible use may result in the loss of my network or Internet access.

Appendix 3

E-safety Consent Form

The Winston Churchill School

Parent/Carer consent form and E-safety Rules

All students use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign agreements to show that the E-safety Rules have been understood and agreed.

Parent / Carer name: ……

Student name: ……..…….

As the parent or legal guardian of the above student, I have read and understood the attached school E-safety rules and grant permission for my daughter or son to have access to use the Internet, school email system, learning platform and other ICT facilities at school.

I know that my daughter or son has signed an E-safety agreement form and that they have a copy of the school E-safety rules. We have discussed this document and my daughter or son agrees to follow the E-safety rules and to support the safe and responsible use of ICT at The Winston Churchill School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching E-safety skills to students.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their E-safety or e-behaviour that they will contact me.

I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's E-safety.

Parent/Guardian signature: ……..

Student signature:……

Date: ……

Further information for parents on E-safety can be found at: http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

Please complete, sign and return to the school secretary.

Appendix 4

E-safety sanctions

It is appropriate for people to be allowed a great deal of freedom in using ICT for study, work and leisure. With freedom comes responsibility. The Winston Churchill School cannot control what people, all over the world, make available on the Internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the ICT network.

We expect all ICT users to take responsibility in the following ways:

Not to access or even try to access any material which is:

- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- In breach of the law, including copyright law, data protection, and computer misuse
- Belongs to other users of ICT systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's Internet filtering
- Not to download or even try to download any software without the explicit permission of a member of the ICT systems support department
- Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the ICT Facilities
- To report any breach (deliberate or accidental) of this policy to Subject Leader of ICT immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. The Winston Churchill School reserves the right to access all material stored on its ICT system, including that held in personal areas of staff and student accounts for purposes of ensuring DFE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the ICT facilities. The Winston Churchill School will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the ICT facilities – on a permanent bas

Appendix 5

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

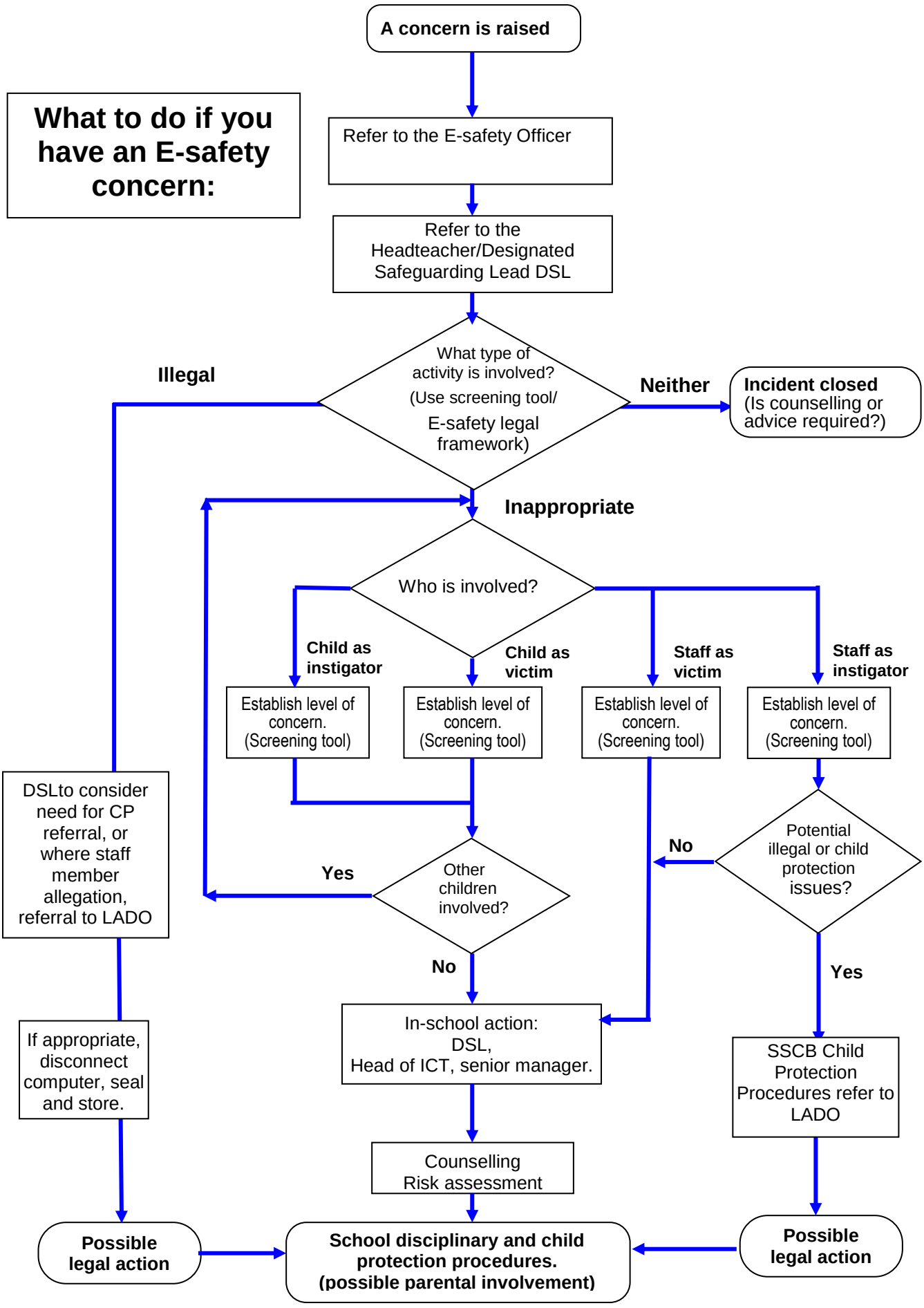
In addition to face-to-face bullying, bullying via technology is becoming increasingly prevalent.

“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’.



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

Screening Tool

This screening tool can be used to assist initial decision-making in dealing with incidents of computer or E-communications misuse within your school. It should be used with the e-Safety flow chart and incidents of misuse matrix.

If you are concerned that a student may have been a victim of a criminal offence or suffered abuse, please consult your DSL who will consider whether to make a referral to social care.

If an adult in school may have committed an offence, consult with the LADO[1] first. Make full records of all information and actions.

Initial questions to consider:

Type of incident

Sexual	□
Bullying	□
Violence	□
Incitement	□
Financial	□
Grooming	□
Other	□

How was the incident discovered?

Self reported	□
Reported by 3rd party (friends or parents)	□
Reported by Teacher or adult in school	□
Other (e.g. Police or Internet Watch foundation)	□

What was the child's response to the incident (if known)?

Unconcerned	□
Curious	□
Distressed	□
Frightened	□
Secretive	□
Other	□

[1] The LADO is the Local Authority Designated Officer in each authority to whom allegations against adults working with children within the scope of the LSCB Child Protection Procedures should be reported. They will give advice and consult police and social care colleagues as appropriate, where a person has:

- behaved in a way that has harmed, or may have harmed, a child
- possibly committed a criminal offence against or related to, a child: or
- behaved towards a child or children in a way that indicates s/he is unsuitable to work with children

The Incident:

1) Who was the victim and who was the instigator?

2) What did the incident refer to?
Answer all questions relating to the particular incident:

CHILD (OR ADULT) AS VICTIM:

Content

1. What was the type of content?
   (Sexual, violence, racial, other)
2. Did anyone else see it?
3. Have they told anyone else about it?

Publishing

1. Is the child/adult identifiable?
2. Can their location be traced/
3. Is text or image potentially indecent or illegal?

Bullying

1. What was the type of bullying?
   (sexual, violent, physical, group)
2. Were information or images published of the child/adult?

In the case of a child: Predation / Grooming

1. Assess the extent of the contact(Consider if an offence has occurred)
   a. One off conversation
   b. Regular conversation
   c. Regular conversation using inappropriate or sexualised language or threats
   d. Attempts to breakaway
   e. Offline meeting arranged
   f. Offline meeting occurred
2. Are the parents aware?
3. When did the incident occur?
4. Did the child give out any personal information?

Action

Once you have gathered the appropriate information, assess the effect of the incident on the child/adult and identify how the person can be best supported. For children, this may be either in school (using existing policies and resources to support children) or where referral to social care is required, and police are involved, support in consultation with them; Witness Support, ACT, CAMHS etc.

For an adult, support within the school's duty of care to include access to employers counselling helpline, action against a child instigator as agreed within the school's Behaviour Management Policy etc

CHILD AS INSTIGATOR:

Content

1. What was the type of content? (sexual, violence, racial, other).
2. Did anyone else see it?
3. Have they told anyone else about it?

Incitement

1. Was the child secretive about the site?
2. Did the child access the site in an isolated place?
3. Did the child understand the risks of accessing this site?
4. Was the child's response to the site?
    - Healthy (e.g. using for research)
    - Problematic (looking for advice or guidance)
    - Harmful (relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites).

Sending/Publishing information

1. Might an offence have taken place?

(Refer to glossary for information on what constitutes an offence).

2. Were others put at risk (e.g. their image / information was sent / published)?
3. Was this an isolated incident or persistent?

Interception of communications / Hacking

1. Has the child placed themselves or others at risk?
2. Has personal or financial information been stolen?

(If yes, this constitutes a criminal offence and advice should be sought from the police).

3. Has illegal content been accessed and sent to other's computers?

Where the Instigator is a child, seek the DSL's assistance to refer to social care following CP Procedures on 0300 200 1006 in cases of sexual abuse, otherwise follow disciplinary penalties as agreed with parents, pupils and staff in the school's Behaviour Management Policy.

If the Instigator is an adult in school, go to next section

ADULT MISUSE/ADULT AS INSTIGATOR

Training

1. Has the member of staff[2] signed an Acceptable Use Policy (AUP)?
2. Had the staff member received training or information on safe practice when using technology during their induction?

Activity

1. Did the member of staff misuse the school's internal email system?
2. Did the member of staff/adult in school, communicate with a young person inappropriately, e.g. via text message, multimedia images, social networking, chat rooms (and see below)
3. Did the member of staff access inappropriate material within school or when using school equipment?
4. Did the member of staff/adult access inappropriate material using their own equipment?

Illegal activity/possible sexual grooming

1. Did the member of staff communicate with a young person inappropriately, e.g. via text message, multimedia images, social networking, chat rooms.
2. Did any communication include the use of inappropriate or sexualised language/threats?
3. Did the member of staff access inappropriate/ illegal material anywhere, thought to be child images (under 18)

Action

If the concern is about possible criminal activity by an adult, i.e. involves child pornography or other grooming type behaviours, follow the Surrey Child Protection Procedures (Managing Allegations against Staff) and consult with the Duty LADO on 01372 833310.

If the matter involves viewing adult pornography, or other similar misuse, report to the Head teacher who should follow the school's disciplinary procedure, seeking advice from HR

The LADO is the Local Authority Designated Officer in each authority to whom allegations against adults working with children within the scope of the LSCB Child Protection Procedures should be reported. They will give advice and consult police and social care colleagues as appropriate, where a person has:

- behaved in a way that has harmed, or may have harmed, a child
- possibly committed a criminal offence against or related to, a child: or
- behaved towards a child or children in a way that indicates s/he is unsuitable to work with children

[2] all adults in school are covered in the responsibility to act safely and responsibly around children. Some activities will apply to employed staff only eg misuse of school equipment; volunteers and governors also come under the duty to report to the LADO where they are suspected of inappropriate activity towards children

Appendix 6
Proposed responses to E-safety incidents by children matrix:

The following matrix offers examples of typical incidents and suggestions as to possible responses. The School's Behaviour Policy, agreed with all, should indicate what penalties will apply to misuse.

Child as victim

Child as victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Receiving unsolicited content that is inappropriate, obscene, offensive or threatening	Web sites (often through mis-clicked or mis-typed web addresses); email (Spam); banner advertising; pop-ups (largely eradicated through better browser design).	Educator vigilance; Acceptable Internet Use Policy known by all users, and is enforced by school. Effective web filtering in place. Using safe filtered email. Effective spam filtering. Maintain email and URL logs and history.	Complete a risk assessment to determine severity of impact on the child. As the content is unsolicited, there can be no question of culpability of the child. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Ensure incidents are reported and recorded.	*All secondary children should have access to the Internet and personal email as an entitlement. Protective measures are essential; however it is not acceptable to be so risk averse that access is removed entirely. There should be procedures agreed with parents and Governors for reporting abuse.*

Child as victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Child is the subject of published material.	Images stored in publicly accessible areas; Personal blogs such as MSN spaces, BEBO etc.; Details left on web sites. Incitement: hatred and discrimination, personal harm etc.	Educator vigilance; Acceptable Internet Use Policy known by all users, and children made aware of the dangers.	Complete a risk assessment to determine the severity of impact on the child. Determine if a perpetrator / victim relationship may exist. Where an in-school perpetrator is identified, and a crime has taken place, police should be informed. Disciplinary action may follow. Where an external perpetrator is identified, report to police. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate.	*Most image storage sites have levels of access, usually private; family & friends and public. These sites are great fun for sharing images; however care should be taken, as users may be able to access inappropriate images posted by others.*

Child as victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Bullying and threats.	Email; text messaging; blogs; Instant Messenger. Incitement: hatred and discrimination, personal harm etc.	Reinforcement of school ethos and behaviour. Regular sample trawls of known sites.	Complete a risk assessment to determine the severity of impact on the child. Determine if a perpetrator / victim relationship exists. Where a perpetrator is identified take appropriate disciplinary action. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate.	*There is no real difference between bullying and threats using technology and more familiar means. Bullying and threatening behaviour is damaging and wrong and should be treated very seriously.*
Security	Adware; browser hijack; virus.	Secure and up to date browser settings and anti-virus software; regular adware scans.	Effective reactive technical intervention.	*This is a frequent problem that is amplified where operating systems and browsers are not regularly updated. It can often occur where inappropriate sites have been visited.*
Predation and grooming	Forming online relationships by deception with the intent of gaining the confidence of a minor to do harm.	Teach awareness of dangers. Use the 'Think U Know' teaching resources.	Where a perpetrator is identified takes appropriate disciplinary/legal action, and in the first instance refer to police. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required.	*Grooming and predation is a child protection issue and should be reported to social care/ police in all cases, or referred to the CEOP through their reporting web site.*
Requests for personal information.	‘Phishing' is the use of deceit to obtain personal (usually financial) information.	Teach awareness of dangers.	If identity theft occurs it should be reported to police without exception.	*Most 'phishing' is aimed at adults with banking facilities, so older children are more likely to e affected.*

Child as instigator				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Soliciting content that is inappropriate, obscene, or offensive.	Use of inappropriate search terms; Accessing or forwarding the details of known sites; Following inappropriate links or banners; inappropriate Image searches.	Use safe image search engines. Effective web filtering. Educator vigilance. Effective incident reporting procedures for blocking sites once known.	Inform parents (consider standard letter templates). Restrict computer or Internet access for a fixed period, dependent on severity. Maintain incident records to identity patterns of behaviour. -If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	*Maintain records of incidents to identify serial offenders.*
Sends or publishes content that is inappropriate, obscene, offensive or threatening.	Emails blogs; msn-spaces; social sites (BEBO etc.) Chat rooms.	Block access to specific sites.	Maintain records of incidents to identify regular offenders. Inform parents. (Consider standard letters). Remove computer access for a fixed period. -If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	*The medium is less important than intent. Publishing is easy using the web; however in legal terms it can still be libellous and subject to the same legal remedies. Where there are known sites that do not moderate effectively they should be blocked.*
Identity Theft	Using others identity to gain access to school systems or services.	Systematic changes of password. Alternative methods of authentication, such as swipe card or fingerprint.	Recover identity and change password. Inform parents (standard letter templates). Restrict computer or Internet access for a fixed period, dependent on severity. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required.	*It is essential that schools consider carefully where personal data is stored, and who can access this data. Access to names and addresses must be secure, and CRB checks in place to protect children.*