Eastwick Schools

E Safety Policy

Governors' Committee Responsible: Resources **Status: Statutory**

Review Period: 2 years **Next review Date:** September 2017

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Eastwick Schools we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information and training. As mentioned in this policy it aims to create and maintain a safe online and ICT environment for Eastwick School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

- The school's e-safety Leader are Miss Langley and Mr Follows
- The e-Safety Governor is Lee Saunders
- The e-safety Policy and its implementation shall be reviewed annually.

<u>Roles and Responsibilities</u>

Governors:
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the e-Safety Co-ordinator/Officer.
- Regular monitoring of e-safety incident logs.
- Reporting to the Behaviour & Safety Committee.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community. Day-to-day responsibility for e-safety will be delegated to the e-Safety Leaders.

• The Headteacher/Senior Leaders are responsible for ensuring that the e-safety Coordinators, and other relevant staff, receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues.
• The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net, and also supports colleagues who take on important monitoring roles.
• The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Leaders:

• Take day-to day-responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policy/documents.
• Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• Provide training and advice for staff.
• Liaise with school ICT technical staff.
• Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As a result the school has a duty to provide pupils with quality Internet access as part of their learning experience:
• The school Internet access will be designed expressly for pupil use including appropriate content filtering.
• Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
• As part of the new ICT (computing) curriculum, all year groups are taught digital literacy units that focus on different elements of staying safe on line. These units include topics on use of search engine, digital footprints and cyber bullying.
• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi- ethnic society. We also measure and assess the impact regularly through meetings our SEN co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

• All staff must read and sign the 'Acceptable ICT Use Agreement' (Appendix 3) before using any school ICT resource.
• Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
• Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:
• If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
• Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
• The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety. We achieve this by ensuring:
• Pupils may only use approved e-mail accounts on the school system.
• Pupils must immediately tell a teacher if they receive offensive e-mail.
• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
• Whole class or group e-mail addresses should be used in school rather than individual addresses.
• E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
• Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact. The school takes the following steps:

• Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

• Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

• Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

• Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

• Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded on the E-Safety forms that are kept in the Heads office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require HT intervention (e.g. cyberbullying) should be reported to HT in the same day.

Allegations involving staff should be reported to the Headteachers. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's Designated Officer should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.
The school takes the following steps:

• Pupils can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into their class teacher at 8:45 and collected at the end of the day.
• The sending of abusive or inappropriate text messages is forbidden.
• Staff should always use the school phone to contact parents.
• Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
• Staff may use their mobile phones in the staffroom/one of the school offices.
• Parents cannot use mobile phones on school trips to take pictures of the children

On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred. The school takes the following steps:

• Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
• Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
• Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
• The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera to capture images and should not use their personal devices.
Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

• Contact details on the Website will be the school address, e-mail and telephone number.
• Staff and pupils' personal information will not be published.
• One of the Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
• Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
• Pupils' full names will not be used in association with photographs.
• Consent from parents will be obtained before photographs of pupils are published on the school Website.
• Work will only be published with the permission of the pupil.

• Parents should only upload pictures of their own child/children onto social networking sites.
• The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

• School ICT systems capacity and security will be reviewed regularly.
• Virus protection will be installed and updated regularly.
• Security strategies will be discussed with the Local Authority.
• E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk

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. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

• Complaints of Internet misuse will be dealt with by a senior member of staff.
• Any complaint about staff misuse must be referred to the Headteacher.
• Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
• Pupils and parents will be informed of the complaints procedure.
• Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

• Rules for Internet access will be posted in all Classrooms.
• Pupils will be informed that Internet use will be monitored.
• Pupils will be informed of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

• All staff will be given the School e-safety Policy and its importance explained.

Parents:

• Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Further Resources
We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Appendix 1

Key Stage One agreement for using the computer and other technologies

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

Signed ……

Appendix 1

Key Stage Two agreement for using the computer and other technologies

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (e.g. my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult

that I know with me

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed……

Appendix 2 – Parent letter – Internet/e-mail use

Eastwick Schools

Parent /Guardian name:……..
Pupil name: …….
Pupil's class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment (i.e. The Hubb), school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

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 pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service; secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. 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.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent's signature:…… **Date:**…….

Appendix 3

Staff Acceptable Use Agreement

The School is committed to the development of effective teaching and learning strategies that use ICT in a responsible and socially acceptable fashion to enhance learning. The school wishes to encourage the responsible educational use of Computing Technology as a means of widening and deepening learning. However, the benefits must be accompanied by responsibility and the school will act to protect its community from illegal and undesirable use of this technology. The purpose of this policy is to define the acceptable use of ICT for all members of staff within the school, with particular reference to the use of the internet, email, portable devices and social media.
Please read the School Rules for Responsible ICT shown below and then complete and return this form to the Finance/Admin Manager, taking a copy to refer to.

Overview:

The same standards of acceptability apply to material accessed through ICT as to material in any other form. If unacceptable in a book, magazine, video, audiotape or spoken form. then it is also unacceptable on the ICT network.
The School cannot control what is made available world-wide on the Internet and will take all reasonable steps in conjunction with its Network supplier to restrict access to undesirable sites. However, there are also requirements on all users, because some material may still be accessible that will not be acceptable in school. The school makes no warranties for the network service it provides and will not be responsible for any damages suffered through data loss or for the accuracy of information provided via the Internet.

Requirements on all staff users (teaching and non-teaching):
a) No user should attempt to access or email any material which is:

- violent or which glorifies violence
- criminal, terrorist or which glorifies criminal activity (including drug abuse)
- racist or designed to incite racial hatred
- pornographic
- crude, profane or with otherwise unsuitable language
- blasphemous or mocking of religious beliefs or values
- in breach of the law, including copyright, data protection and computer misuse
- the property of other ICT system users without their explicit permission

b) No user should use the network in the following ways:

- downloading software without the permission of IT staff
- downloading inappropriate material (as defined above)
- using chat lines except for subject use (e.g. languages)
- sending frivolous or malicious messages
- giving out personal details of themselves or others in emails to strangers
- lending passwords or using other people's passwords
- Attempting to access any part of the school's network operating systems (unless authorised to do so)
- loading and using software programmes brought in from outside school

c) When using portable devices outside of school users should;

- only use them for school/work use
- not keep personal information, files or photos on them
- not leave the device unattended in cars or vulnerable places
- have suitable insurance to replace lost, stolen or damaged items

d) The use of social media
With the increase in the availability of social media we have a duty to safeguard the children within the school but also ourselves and the school in the online community.
Staff who work within the school and use social media;

- should not engage with current students or parents via social media
- should ensure that their privacy settings are set to the highest level
- report any communications from students to the child protection officers
- report any information they receive about inappropriate use of social media by students to the child protection officer
- should report any inappropriate comments about the school or staff to a member of the SLT
- should not post anything specific to children or the school that may affect the reputation of the school
- should remember only to use the school email address

……

Member of staff:

I have read and understand the School Rules for responsible ICT Use, and agree to comply with them. I will use the Internet, and other ICT facilities at school in a safe and responsible way and observe all the restrictions explained to me by the school. I understand that the school will take reasonable precautions to ensure that pupils cannot access inappropriate materials, including the teaching of Internet safety
skills to pupils. Whilst I acknowledge that pupils will be deemed to be accountable for their own actions, I accept that when using ICT within school:

- I accept responsibility for setting and conveying standards for pupils to follow when selecting, sharing and exploring information and media

- I must monitor the nature and content of materials accessed through the Internet.

Staff signature: _____

Staff name:_____Date: _____

Information for 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

Cyberbullying

In addition to face-to-face bullying, bullying via technology is becoming increasingly prevalent. "Cyberbullying" is the use of Information and Communications Technology, ICT, particularly mobile phones and the internet, deliberately to upset someone else. "Cyberbullying" 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.

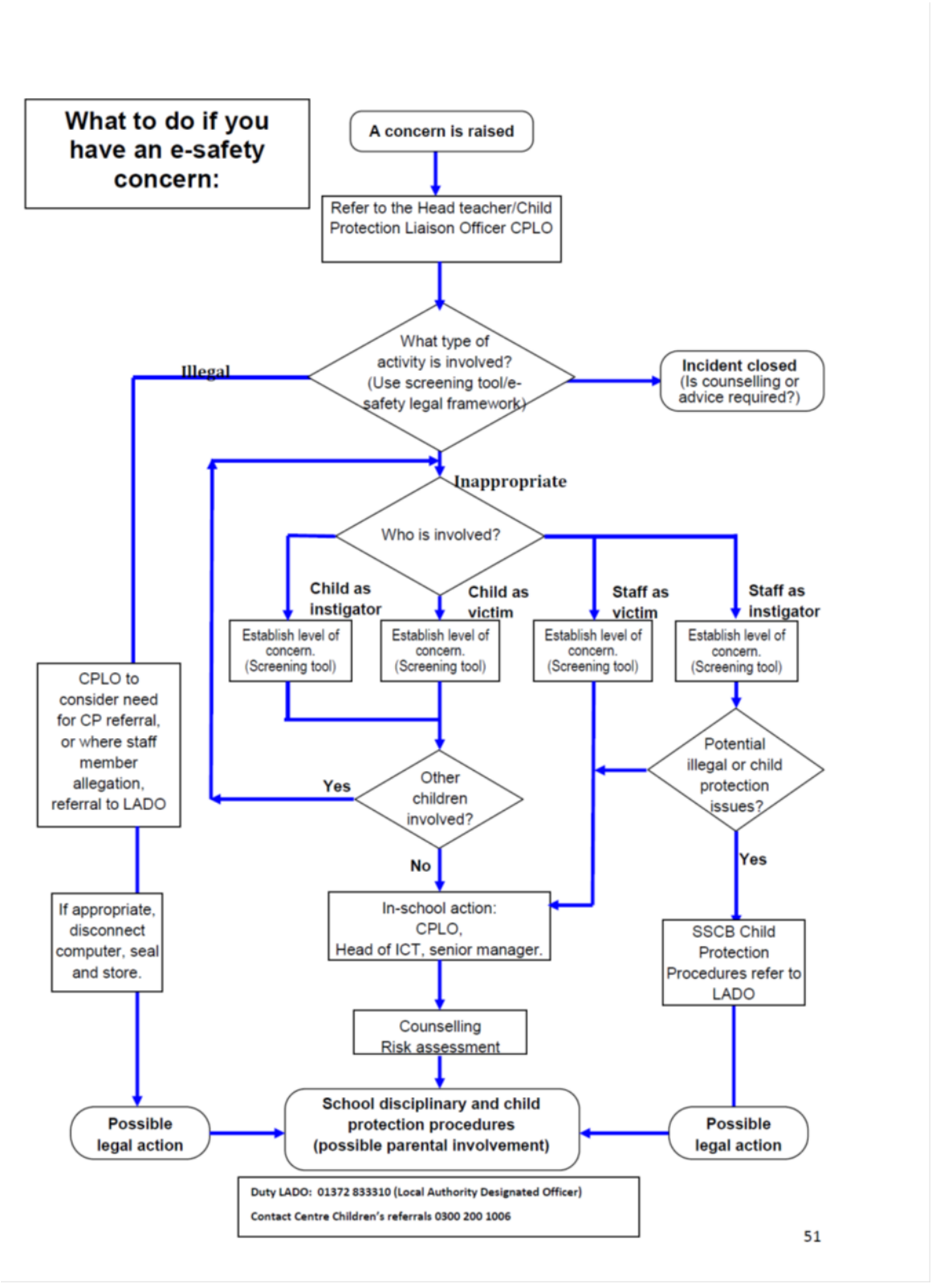
Inappropriate or illegal content

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'.

Appendix 4


What to do if you have an e-safety concern:
A concern is raised
Refer to the Head teacher/Child Protection Liaison Officer CPLO
What type of activity is involved? (Use screening tool/e-safety legal framework)
Illegal
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
CPLO to consider need for CP referral, or where staff member allegation, referral to LADO
Other children involved?
Yes
No
Potential illegal or child protection issues?
Yes
If appropriate, disconnect computer, seal and store.
In-school action: CPLO, Head of ICT, senior manager.
SSCB Child Protection Procedures refer to LADO
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures (possible parental involvement)
Possible legal action
Duty LADO: 01372 833310 (Local Authority Designated Officer)
Contact Centre Children's referrals 0300 200 1006
51