ANGLO EUROPEAN SCHOOL

E-SAFETY POLICY

Policy	
Received/first adopted*	December 2011
Origin	AES
Statutory/Non-Statutory	Non Statutory
Reviewed/Approved * by Leadership Team	01/10/16
Ratified/Reviewed* by GB Committee Curriculum/Finance/Personnel*	Personnel 04/10/2016
Ratified/Reviewed by FGB	Noted 07/12/2016
Published to Governor's area on Website	11/10/2016
Published in school	11/10/2016
Planned review date if any	04/10/2017
Reviewed	Annually

**Delete as applicable*

ANGLO EUROPEAN SCHOOL – E-Safety Policy – September 2016

INTRODUCTION AND ETHOS

Anglo European School is committed to promoting the safety and well being of our staff and students. We are committed to using new and emerging technologies to drive forward education and use technology to help to deliver a creative and educationally stimulating balanced curriculum. We are appreciative of the wealth of information which the use of these technologies can bring to aid teaching and learning. With this in mind, we are knowledgeable about the potential hazards, dilemmas and dangers which our community may face when using new technologies.

E-POLICY AIMS & OBJECTIVES

Aim: To ensure that members of our school community are safe, knowledgeable and responsible users of e-technology.

Our specific objectives are as follows:

1. The need for care when inputting personal information, or when using the internet
2. To make staff and students aware of the need for safe-guarding themselves when using new and emerging technologies
3. To provide and promote opportunities to raise staff and students awareness of new and emerging technologies
4. To use new and emerging technologies to actively support the curriculum
5. To support parents in protecting their children when using the technology they have

WHY IS E-SAFETY IMPORTANT?

- **99%** of our school children live in a household with Internet
- Nationally, 55% access the internet **everyday**, 47% for an hour or more

- **34% of children aged 8-12 have a profile on sites that require users to register as being 13 or over**
  21% liked IM/Chat the most
  15% used gaming sites
  11% used social networking sites
  33% had access in their bedrooms

- **40% of KS3 and 4 students nationally are known to have witnessed a 'sexting' incident** and in the same group, 40% didn't consider topless images as inappropriate

- **25% have met someone offline – one quarter of these did not take anyone with them**

- **Of the three quarters who did, 83% took a friend not a trusted adult.**

Younger children are increasingly using social networking sites as evidenced by the rise of usage by those aged 5-7 in the UK from 7% in 2009 to 23% in 2010. This is largely driven by sites like Club Penguin and Moshi Monsters rather than age-restricted sites like Facebook. However, Facebook remains enormously popular (96% of those aged 8-15 with an active social networking site profile use Facebook) and

there are a significant number of underage users accessing sites like Facebook which have a minimum user age of 13. In the UK, it seems that starting with secondary school at the age of 11 is a key trigger for underage social networking: 28% of those aged 9-10 have an SNS profile compared to 59% of those aged 11-12. However, safety campaigns do seem to be successful: although those aged 9-12 are the most likely in Europe to display an incorrect age, they also the most likely to keep their profile private.

EQUAL OPPORTUNITIES

Anglo European School is committed to ensuring that technology, information, advice and guidance is available to and accessible by all. 99% of our students have internet access at home. All students have supervised access to the internet at school via study club. The school uses the RM filtering service.

STAFF RESPONSIBILITY & DEVELOPMENT

Designated Safeguarding Lead – Ruth Wootton
Assistant Designated Safeguarding Leads – Darren Priestley/Nikki Foster
Senior Link to ICT Technical Department – Graham Headley

The ICT Technical Team are available to offer guidance and support on the use of new and emerging technologies and software. A training programme for the use of new resources will be put in place as and when required.

The school supports staff CPD opportunities on the use of new and emerging technologies which promotes high quality teaching and learning. Any member of staff wishing to apply for training offered by an external provider will need to complete the Inset Request Form and submit to Assistant Head teacher with responsibility for CPD.

INTERNET AND THE LAW

In many cases, laws relating to copyright, libel, or incitement to racial hatred apply to the use of the internet as they would for any other forms of communication. Child Protection legislation applies as do relevant laws on obscenity and indecency. Criminal charges can result from the misuse of the internet and teachers have a duty to provide protection for the students in their care.

The school adheres to the Computer Misuses Act which recognises the following offences:

- Gaining unauthorised access to computer material, for example, guessing someone's password, then using it to access a computer system and looking at or altering the data it contains.
- The intentional modification of computer material including deleting files, changing the desktop set-up or sending computer viruses with the intent to disrupt.

SHOW MY HOMEWORK

This is an effective tool to communicate to both the students and their parents about homework which has been set.

This web based resource can be accessed by the student/parents at any time. Staff should do their best to ensure that spelling, punctuation and grammar are correct on.

Personal password protection

Great care must be taken to ensure personal passwords remain confidential – if it is felt that a student has obtained a teacher's password, the ICT Network Manager must be informed immediately and the password reset.

Downloading software

Downloading software and other data from the internet onto the school network or hard drive should be undertaken only by the ICT team. The sixth form block has WIFi access and the school uses Ruckus Zonedirector and onBoarder systems as well as Lightspeed to enable the schools filtering systems to be fully implemented.

E-MAILS

Staff

The school are aware that e-mail can be an effective method to communicate with members of the school's staff and via the use of Parentmail to convey information to parents. However, it is acknowledged that e-mails can be misinterpreted and staff ***should not*** enter into e-mail communications with parents regarding their child's progress. Year Leaders and the SEANCO have the permission of the Headteachers to use emails to communicate factual information to parents.

Parents

In the event that a parent contacts a member of staff via e-mail, the member of staff must ask the school office to send an e-mail via feedback acknowledging receipt. Traditional method of communication must be used to respond.

In the rare event that it is felt necessary to use e-mail as a method of communication with parents, this must be on agreement with the Senior Link and staff must use their school e-mail address. Copies of correspondence must be kept in the students file.

In every case, e-mails should be confined to 'facts' rather than giving 'judgements' or 'criticisms'.

Students

The school acknowledges that e-mail can be an effective method to communicate information related to school matters to students. In such instances, staff must use both their, and the students school e-mail address and send a copy to the Head of Department. If there is a need to use any other e-mail address, this must be pre-agreed with the Senior Link and the parents informed. In every case, e-mails should be confined to 'facts' and not give 'judgements' or 'criticisms'.

The actions of all users of the internet are durable and can be traced. Internet users leave a record in the browser of everything they have looked at and of all e-mails sent

and received. If inappropriate material is inadvertently accessed or received by students or staff, this must be reported immediately to a Deputy Head teacher or Headteacher.

USE OF WEBCAMS

The school is aware of the benefits which communicating using webcams can have. Staff must ensure that they go through the procedures for using webcams (as stated in the ICT Acceptable Use Policy) with the students. Webcams should only be used in scheduled lesson time and as part of the planned curriculum activity under teacher supervision.

COMMUNITY USE

When ICT resources are used by the community, it is the event organiser's responsibility to make the group members aware of the school's e-safety policy and ICT Acceptable Use Policy. Any contravention to this must be reported to a Deputy Head teacher.

CYBER BULLYING

Cyber bullying can be defined as the use of *Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.* It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying, namely:

- the invasion of home and personal space
- the difficulty in controlling electronically circulated messages
- the size of the audience
- the perceived anonymity

Cyber Bullying can be 24/7 and can also affect members of school staff and other adults; where staff can be ridiculed, threatened and otherwise abused online by students.

Cyber Bullying can take different forms such as: threats and intimidation; harassment or "cyber-stalking" (e.g. repeatedly sending unwanted texts or instant messages); vilification / defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images); and manipulation.

If staff feel that a student is the target of cyber bullying, they should ask them to save and print out the dubious or worrying material and make a referral to the Year Leader, together with this evidence and a student statement. The Year Leader will refer the investigation to the Assistant Head teacher - Community. In extreme circumstances, the school will make a referral to the police or CEOP (Child Exploitation and Online Protection), if deemed appropriate.

SOCIAL NETWORKING SITES inc TWITTER

Staff

Before participating in any online community:

- staff must remember that anything posted online is available to ***anyone in the world***

- **a**ny text or photo placed online becomes the property of the site(s) and is completely out of our control the moment it is placed online – ***even if access to your site is limited***
- Staff are reminded of the need for discretion and professionalism when up-loading data which could potentially have a negative impact on the school or individual concerned. Such action could lead to disciplinary procedures being instigated.
- Staff ***should not*** add ***current students*** to or become members of students' social networking sites
- Staff have a duty of care to our young people and must not put themselves in situations which could potentially comprise their professionalism
- Staff must also be aware that ex-students may also have current students as members of their social networking sites. To this effect, staff are ***strongly advised*** not to post personal details such as address and telephone numbers etc when setting up a social networking account
- Remember, photos of you can be posted by others and tagged.
- Pornographic sites should not be accessed under any circumstances. Any teacher who uses school internet facilities to download pornographic materials is likely to be judged as committing an act of gross misconduct.
- Access to other offensive or inappropriate sites should also be avoided. There may be circumstances where access to such material is necessary to inform teaching and learning. In such cases, prior permission from the Deputy Headteacher (Designated Safeguarding Lead) is needed.
- Chat rooms should not be accessed in school, for either professional or personal purposes, without obtaining prior permission from the Deputy Headteacher (Designated Safeguarding Lead).
- No student or member of staff should post images or video footage of the school, staff, students or the school's name on any internet site, without prior written consent from the Headteachers.

In practical terms, the following are essential when dealing with offensive posts or tweets:

1. The school will not rely on second hand information about what has been written. We will aim to see and keep a hard copy of the evidence.
2. Once we have obtained the hard copy, we will follow our anti-bullying policy. Some young people do not understand that everyone can read their tweets or posts and they generally agree to remove them when the school asks them to do so. If a young person refuses, the school may contact Facebook and request that the offending post is removed.
3. If the incident reaches an impass and the school considers that the post amounts to criminal behaviour, the school will report the incident to the police.
4. Tweets or Facebook posts can attract press attention. If this occurs, the school may refer to the Councils Press office before replying to any queries.

FRAPPING

This is the unauthorised use of another person's Facebook (or other social networking site). Frapping is classed as the stealing of another person's Facebook (or other social

networking) site. The Frapper may post inappropriate, silly or harmful messages on the person's site. Staff should not engage in Frapping. If a student or member of staff becomes a victim of Frapping then they must refer this to the Assistant Headteacher – Community.

GROOMING

Child grooming refers to actions deliberately undertaken by another with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual abuse or potential radicalisation.

Chat rooms and other social networking sites, are a prime environment where grooming or radicalisation can occur. Chat rooms are filtered in school and should not be accessed by the students. If a member of staff sees a student using a chat room during a lesson, a referral must be made to the Head of Department or to the Year Leader (if the incident occurs outside of a lesson). They will then lead the investigation.

The school is aware that students may use chat rooms at home and we try as far as is reasonably possible to inform students of how to protect themselves. We also aim to inform parents of how to protect their children. Students sometimes speak to staff about the friends who they have made – including 'virtual friends'. Possible warning signs to look for that a student may be being groomed are:

- If the child tells you that their 'friend' is insisting on having their address or phone number.
- If the child states that their friend has emailed them pictures which made them feel uncomfortable and they would not be able to show to anyone else.
- If the child mentions that they have been asked to email their 'friend' pictures of the themselves or use a webcam in a way which makes them feel uncomfortable.
- If the child mentions that their 'friend' has asked them to keep their chats secret.
- If the child says that their 'friend' has said that they will get in trouble if they tell an adult what has been going on.
- If the child says that their 'friend' wants to meet them and tells them not to let anyone know.
- If the child starts to communicate in a very different manner to their 'norm'

In all these situations, recommend to the child that they cease to have any further contact with their 'friend' and make an immediate referral to the Deputy Head teacher responsible for Child Protection, who will make a decision as to whether a referral to CEOP and The Essex Safe Guarding Team is required.

SEXTING

This where a person takes an inappropriate image and sends it to someone or posts it on the social networking site. It may also involve the posting of an image as a profile picture on a social networking site or as a profile picture. These images are then shared with others. If a student or member of staff is aware of issues of sexting then they must refer this to the Designated Safeguarding Lead(s).

SMART MOBILE PHONES

There is the facility to 'Broadcast' the contacts on your mobile phone to everyone on your contact list. This can result in young people being contacted by people that they do not know, as they are friends with someone who the child has on their contact list. Profile images can also be 'munched' (screen shot from another users' Blackberry phone) and sent to those on your contact list.

BLOGGING

The school is aware and supportive of the benefits that BLOGGING can have as a research tool. BLOGS should only be used as part of the structured curriculum and for a pre-determined period of time. It will be the responsibility of the teacher initiating the BLOG to monitor its content. The teacher must remind the students of the ICT Acceptable Use Policy prior to using BLOGS. Any inappropriate use of the BLOG by the students will result in the appropriate action being taken. If a student or member of staff is aware of inappropriate comments on a BLOG then they must refer this to the Assistant Headteacher – Community.

PHISHING

Recent phisihing techniques have taken the form of fraudulent emails from banks stating that account holders need to change their password. Such emails should be deleted immediately.

If a student mentions that they have received a scam e-mail, ask them to print out the e-mail and refer it to the ICT Manager for investigation. Tell the students ***not to reply*** to it because then the fraudsters know that this is an active email address and they likely to be targeted by more fraudsters.

MOBILE PHONES

Mobile phones ***are not permitted*** to be used on the school premises. Staff must refer to the Visits Policy for usage of mobile phones on a school visit.

Mobile phones ***must not*** be used to take photographs in school. It is very easy for students to create, manipulate and circulate inappropriate content. Once forwarded, content is almost impossible to control, and can easily spread by being passed on. Such content is a common form of Cyberbullying.

Staff home phone or mobile numbers should not be given to parents of students – other than for the purpose of the schools visits programme.

PROMOTION OF E-SAFETY

The school will use the following strategies to raise awareness of e-safety.

- Internet Safety Week
- Assemblies
- Publication of the e-policy policy and additional guidance on the school website
- The CEOP Report Abuse Button is displayed on the school website
- Information, advice and guidance is shared with parents

- New staff induction programme
- All our staff (teaching and non teaching) are trained as to how to recognise e-safety issues and how to report them,
- E-safety is addressed in the schools ICT Acceptable Use Policy

MONITORING & EVALUATION

The Deputy Headteacher responsible for Safeguarding will have lead responsibility for the monitoring of e-policy in the school. The impact of the policy will be measured in line with the objectives by:

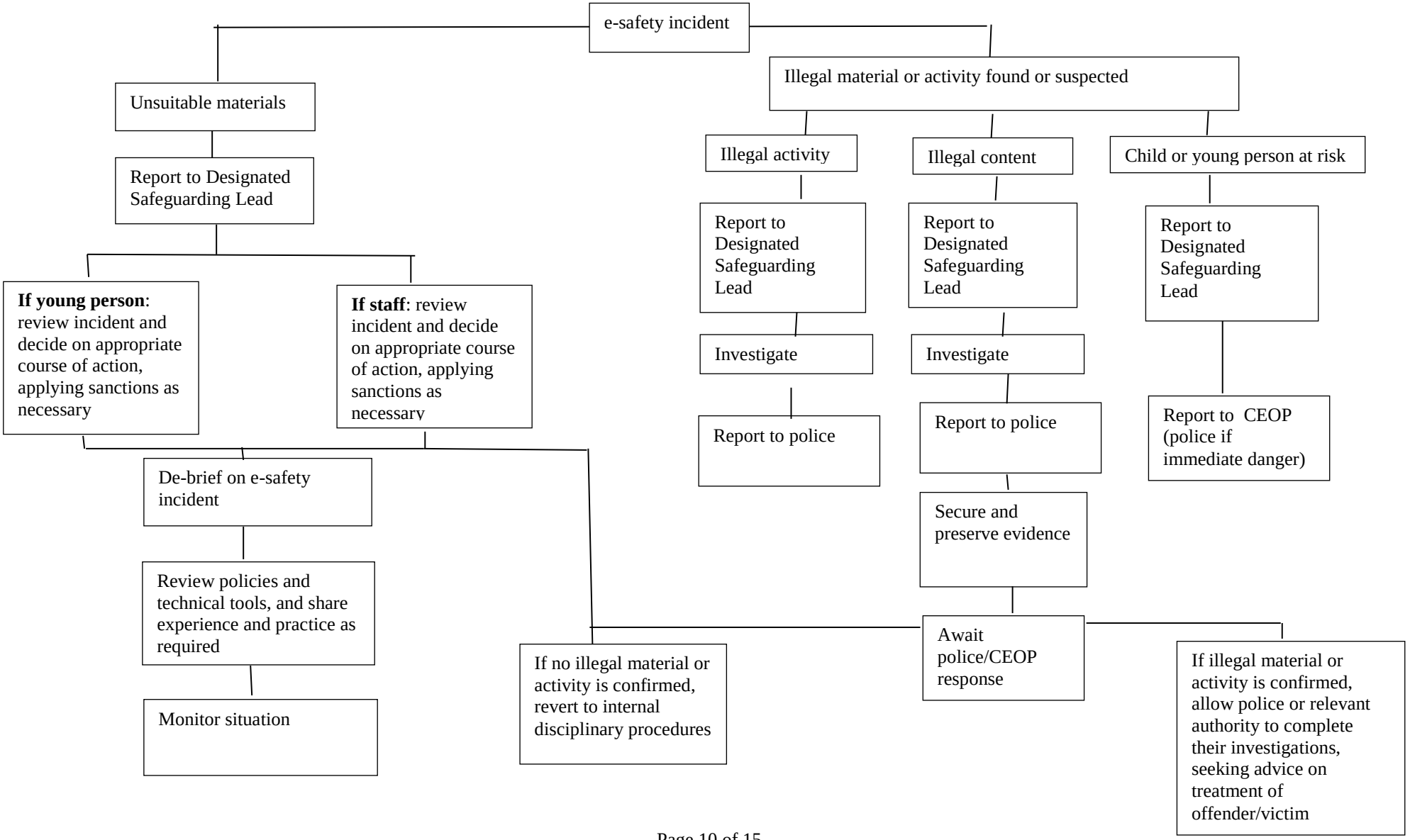
- Spot checks using RM Tutor to monitor ICT activity cross the school
- Keeping a log of and monitoring incidents of misuse and conduct
- Working in partnership with parents to encourage consistency with the implementation of the e-policy at home

PROCEDURES FOR CAUSES FOR CONCERN

If you feel that a student is in any way vulnerable then a referral must be made immediately to the Deputy Headteacher responsible for Child Protection or the Assistant Child Protection Officer.

If a member of staff is in anyway subject to allegation, they must report this to the Hedteachers and they are strongly advised to contact their professional association.

Flowchart for responding to e-safety incidents



For information, the following organisations are available to offer support if needed. However with a school related issue, it would be for the Deputy Headteacher responsible for Child Protection to make a referral to these bodies if deemed appropriate.

Issue	Support	Contact Details
Adult concern of child at risk	NSPCC	0808 800 5000
Adult concern of child at risk	Local Police	Contact your local police station
Adult concern of child at risk	Police Emergency	999
Adult concern of child at risk	Stop It Now! (an organisation that helps tackle child sexual abuse, targeting adults to act responsibly)	0808 1000 900
Adult concern of child at risk	CEOP (Child Exploitation and On-Line Protection Service)	0870 000 3344
Child concern	Child Line	0800 1111
Child concern	There4me (NSPCC's confidential website)	www.there4me.com

USEFUL DOCUMENTS

Communications Market Report: UK Ofcom, 2011
http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK-CMR_2011_FINAL.pdf

Risks and safety for children on the internet: the UK report, LSE, 2010;
http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf

UK Children's Media Literacy, Ofcom, 2011
http://stakeholders.ofcom.org.uk/binaries/research/media-leteracy/media-lit11/childrens.pdf

UK Children's Media Literacy, Ofcom 2011
http://stakeholders.ofcom.org.uk/binaries/research/medi-literacy/media-lit11/childrens.pdf

EU Kids Online II, LSE, 2011;
http://www2.Ise.ac.uk/media@Ise/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)EUKidsOnlineIIReports/Final%20report.pdf

Risks and safety for children on the internet: the UK report, LSE, 2010;
http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf

UK Children's Media Literacy, Ofcom, 2011
http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit11/childrens.pdf

EU Kids Online II, LSE, 2011;
http://www2.Ise.ac.uk/media@Ise/research/EUKidsOnline/EU%20Kids"20II%20

Lack of Internet access puts poorest children at educational disadvantage, TES, 2010;
http://www.tes.co.uk/article.aspx?storycode=6036318

Survive and Thrive, RaceOnline, 2011;
http://www.raceonline2012.org/sites/default/files/resources/survive_thrive_charity_sustainability_through_technology.pdf

Risks and safety for children on the internet: the UK report, LSE, 2010;
http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf

UK Children's Media Literacy, Ofcom, 2011;
http://stakeholders.ofcom.org.uk/binaires/research/media-literacy/media-lit11/childrens.pdf

Risks and safety for children on the internet: the UK report, LSE, 2010;
http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf

Social networking, age and privacy, LSE, 2011;
http://eprings.lse.ac.uk/35849/1/social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/.

In addition, the following terms are useful to support aware of e-safety issues:

360 Degree Safe	SWGfL's online self-review tool for school improvement in online safety www.360safe.org.uk
Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need (commonly used providers include Smoothwall, Lightspeed, Netsweeper, RM).
AUP	Acceptable Use Policy
Byron Review	Professor Tanya Byron's seminal report from 2008, 'Safer Children in a Digital World'.
CEOP	Child Exploitation and Online Protection centre.
Cyber Bullying	Bullying using technology such as computers and mobile phones.
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
EPICT	European Pedagogical ICT Accreditation.
E-Safety Mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor
Frapping	Short for 'Facebook rape', referring to when a Facebook user's identify and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, Playstation 3, Nintendo DS.
Grooming	Online grooming is defined by the UK Home office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
Lifestyle Website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked Down System	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).

Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed System	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed system have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the emails have links in them which take people to fake sites setup to look like the real thing, where passwords and account details can be stolen.
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SHARP	Example of an anonymous online reporting mechanism (Self Help and Reporting Process)
SNS	Social Networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make fiends and stay in touch with people.
Spam	An email message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UC) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
Youtube	Social networking site where users can upload, publish and share video.

Appendix

In the UK, 78% of households now have home internet access, rising to 91% in households with children. In addition, 91% of UK children aged 9-16 go online at school (compared to the European average of 63%), with a significant minority of young people only accessing the internet at school (10% of those aged 12-15). Despite these high levels of internet take-up among families and in schools, 8% of young people aged 5-15 in the UK do not use the internet at all in any location.

- Research by EU Kids Online finds that 'Internet use is increasingly individualised, privatised and mobile' and this is particularly true for the UK. This make education and awareness interventions and materials critical, as children need to be empowered to make good decisions whenever and

wherever they are using the internet. Compared to their European counterparts, UK children are more likely to access the internet from laptops, televisions, mobile phones, handheld devices and games consoles, and on average use 3.5 different devices to go online across four locations.

- According to Ofcom (2011), many young children have unsupervised access to the internet, with a significant proportion of users mostly using the internet on their own (10% of those aged 5-7, 25% of those aged 8-11 and 50% of those aged 12-15). However, since 2010, children aged 5-15 are in fact less likely to use the internet on their own (32% v 36%) and more likely to use it in the presence of an adult (59% v 55%).

- Ofcom has revealed that in 2010, smartphone ownership reached 3% of those aged 5-7, 13% of those aged 8-11 and 35% of those aged 12-15 in the UK. By 2011, almost half of all young people aged 12-15 had a smartphone (47%). 90% of children aged 5-15 in the UK live in a household with a fixed or portable games console. This is often in a private location: nearly 50% of children aged 5-7 have a games console in their bedroom, rising to 70% of those aged 8-15.

- These devices are increasingly used to access the internet and play against others online: 20% of children aged 8-11 and nearly 25% of those aged 12-15 go online using a games console. Of boys aged 12-15 who play games, 19% say they mostly play with other people over the internet.

- The EU Kids Online project shows that school work is the top online activity for UK youth (92% of those aged 9-16) and **more than half of UK teachers believe that children with no internet access are seriously disadvantaged in their education** (TES, 2010). RaceOnline evidence demonstrates that children with Internet access at home attain higher exam results by two grades.

- After schoolwork, playing games is the second most popular activity (83% of those aged 9-16), followed by watching video clips (75% of those aged 9-16) and visiting social networking sites (71% of those aged 9-16).[26] Games are particularly popular with younger children, and it is often through games that children first start to use technology. Just over 33% of those aged 8-11 in the UK visit sites like YouTube, rising to 66% of those aged 12-15 (Ofcom, 2011).