The SENAD Group

Section 5

E-Safety Policy

Issue: December 2016
Reviewed: December 2016
Next Review: December 2017
Version: 6
Policy Ref: 510.0
Owners: BV

The Acceptable Use of the Internet and Related Technologies Policy

APPLICATION

This policy is actively linked to SENAD's Safeguarding Policies and the SENAD Computer, email and internet use company rules and guidelines.

The e-Safety Policy references and is linked to other policies including those for:

- ICT, Anti bullying **502**,
- for Safeguarding **506A A(adults), 506C (children),**
- **PREVENT for anti-radicalisation (506.8)**
- **524** Significant Harm.
- Staff should refer to Policy **402** for guidance of their use of computers and the internet.

A glossary of terms is appended to this document (App. 4)

The Head of Service will identify the E safety Co-ordinator for the SENAD site, who will liaise with the Safeguarding Coordinator on E-Safety issues. The Head of site/Registered Manager and E-safety Co-ordinator will be responsible for defining the site/ Local Acceptable Internet use Guidelines.

This policy applies to Children's Homes, Schools and Adult Homes.

It applies to SENAD Community in that when service users use a SENAD facility, the policy applies, as it also does to SENAD Community employees.

POLICY

Access to the internet is an important aspect of the lives of young people through various devices, Mainstream schools are recognising that the traditional 'Locked down' system of Internet use is unmanageable as a control measure to protect young people from the negative aspects of internet use. The SENAD Group also has this

view and seeks to mirror the approaches taken by these schools in addressing the dangers, yet allowing through a managed approach access to the Internet.

The SENAD Group also recognises that young people with Special Educational needs are more likely to be victims of online abuse, compared with young people attending mainstream Schools; therefore any change from the traditional systems will need to be approached with caution and continual monitoring.

There will be a transition to a Managed System. The ultimate aim will be to help the young people to become safe and responsible users of new technologies.

It should be noted that due to the nature of the young people at some sites the general guidelines below may not be appropriate (for example young people with sexualised behaviours). Free access to the Internet may be strictly controlled as part of their individual Risk Assessment or part of a reward system. This should be covered by site specific policy.

During the transition stage each site will:-

- Work closely with families to help them ensure the young people use new technologies safely and responsibly both at home and at schools
- Use parents, student and residents views to develop the e safety strategies
- Manage the strategic change to help staff and the young people understand how to manage the risks associated with the internet, to protect and educate them in the use of the technologies.
- The transition will recognise the abilities and understanding of the young people at each site, therefore an individual approach will be used for each student and resident.

This Policy aims to address the issues within E-safety which can be categorised in to three areas of risk:-

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users

- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Throughout the policy where it says *'young person'* this is used as a generic term for ANY SENAD service user in a school, children's home or adult home registered with CQC.

Procedure and Guidance

1. Teaching and learning and use by adult service users

1.1 Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and young people. (See policy **701**)

Schools have a duty to provide young people with appropriate Internet access (but not unrestricted nor unaffordable) as part of their learning experience, this is equally as important for our children's homes in the continuing development of individuals, however, parents and young people should be aware that access to the internet outside of education may not be provided or may be withdrawn on specific sites depending on the needs and behaviours of the young people.

Likewise, **our adult service** users will need to have appropriate access to the internet and safeguarding is important in these settings due to our clients' vulnerability.

1.2 Internet use will enhance learning

School Internet access will be designed expressly for student use and will include filtering appropriate to the age of the young people. Where sites have access to multiple levels of filtering, varying levels of access may be provided based on age or understanding of safe internet use. Where a site only has access to a single level of filtering, filtering must remain appropriate for the youngest service users on site.

Young people will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. An example of acceptable programmes of study is *Safe* delivered via the *Makewav.es* educational social networking site platform

Due to the nature of the young people some sites may choose to impose site specific consequences for proven misuse of the internet, these consequences should be defined in a site specific policy. Staff are advised to refer to "The Use of Sanctions", Policy **520.**

Adults will be supported in the appropriate use of the internet.

1.3 Young People and Adults will be taught how to evaluate Internet content

Sites will ensure that the use of Internet derived materials by staff and young people and adults complies with copyright law.

Students will be taught how to report unpleasant Internet content as part of the PSHCE and ICT curriculum and how to use the schools Safeguarding Procedure. Staff will advocate on behalf of students who are unable to do this.

Adult service users will also be made aware of cyber-safety and how to report unpleasant internet content.

1.4 Video and Photo Sharing sites

Students and adults will have a natural and understandable interest in Video Sharing sites for example YouTube. A number of websites use feedback from users to report offensive material. Where content filtering is in use, this will take place based on the text appearing on the page – no software is available that is capable of accurately scanning video content and identifying inappropriate material. This means that an age appropriate video with an inappropriate comment may be blocked whilst an age or content inappropriate video with an innocuous name may slip through.

This can only be managed through supervision, and discussion with a student or resident. Staff will need to react to students or adult *'off the cuff'* remarks particularly around sites that may contain offensive material for example hate, extreme religious, or homophobic material.

1.5 PREVENT - addressing anti-radicalisation

The internet and social media allows service users to be groomed and exposed to radicalisation messages. SENAD's anti-radicalisation policy (506.8) is important here.

We recognise we are in an important position to identify the early signs, looking to safeguard and protect children / young people who are susceptible and vulnerable. We recognise the need to respond in taking appropriate action to prevent extremist views and ideologies developing alongside providing a broad curriculum and appropriate access to the internet for adults in our homes.

In the community, SENAD Community staff will also be aware of radicalisation issues in service users' homes.

Where SENAD staff become aware of a potential issue, then they must follow the golden rule in safeguarding, namely:

"if in doubt tell someone"

2 Managing Internet Access

2.1 Information system security

ICT systems security will be reviewed regularly.

Site antivirus protection will be updated regularly.

Any student or residents devices connected to the site network must have antivirus software installed. SENAD reserves the right to refuse to connect or remove the connection for specific devices to any site network based on security concerns.

2.2 E-mail (Contact)

Young people may only use site approved e-mail accounts on the school system

Young people must immediately tell a member of staff if they receive offensive e-mail.

In e-mail communication, young people must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

In the home setting young people and adults will be encouraged to make informed decisions on E mail content.

2.3 Published content and the school web site

Staff or student personal contact information will not be published. The contact details given online should be the school office.

2.4 Publishing Young people and Adults images and work

Issue of Consent:

The Data Protection Act 1998 affects our use of photography. Written parental/carer consent must be obtained before taking photographs or making video recordings of students. Consent forms are available for this purpose.

Consent for photography or video recording is sought when a young person is admitted and lasts for the duration of their stay. Parents of young people retain the right to withdraw consent in writing at any stage.

In the Public Domain:

Images of Young people and adults must not be used anywhere on a public school Web site or other public on-line space or in publications. Exceptions must be approved by the Head teacher and written consent obtained from parents/carers.

Internally:

With written parental/carer consent, images and videos may be taken and stored for evidence towards accreditation and records of achievement i.e. for showing at annual reviews. Note SENAD equipment must be used. Personal equipment must not be used for this purpose, for example personal cameras, mobile phones, electronic storage devices or any type of photographic equipment.

2.5 Social networking and personal publishing

The sites will manage access to social networking websites, and consider how to educate young people in their safe use. SENAD sites will approve access on an individual basis to social networking based

on age appropriateness and subject to a decision from the sites E-safety coordinator and Registered Manager/Site Head.

The school will use an accepted educational platform for teaching digital citizenship and E-safety online for example the Makewav.es website in conjunction with the *Safe* programme of study – parental consent will be sought before delivering the *Safe* programme of study to students.

Specific social networking sites and newsgroups may be restricted due to them being age inappropriate, an age restriction set by the website, or content, unless a specific use is approved and parental permission obtained. Individual use may be managed following discussion with Parents, Head of Site or Registered Manager.

Young people will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Ideally young people would use only moderated social networking sites, e.g. SuperClubs Plus.

Young people and parents will be advised that the use of social network spaces outside school brings a range of dangers for young people as an example frape where the victim's identity is compromised, or online grooming. Staff are advised to refer to Policy **502** Anti bullying.

Young people will be advised to use nicknames and avatars when using social networking sites.

Staff should refer to HR Policy **402** "Computer, Email and Internet Use" Policy when using social networks, in particular comments placed on the sites.

2.6 Managing filtering

Sites will use age appropriate internet filtering plus additional filtering/monitoring on individual machines based on specific needs as required to protect young people.

If staff or young people identify unsuitable on-line materials, the website must be reported to the E-Safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.7 Managing videoconferencing & webcam use (including Skype)

Videoconferencing, Skype and webcam use will be approved following a specific request from either Parent/carer or the young person and agreed by the school and written parental permission obtained.

Young people must ask permission from a senior member of staff, residential house manager/teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised for the pupil's age, and level of understanding.

Young people must not use video based conferencing in an area where other young people may appear in the video without their or their parents' consent (where appropriate)

2.8 Managing emerging technologies

Emerging technologies will be examined for educational benefit and an individual risk assessment will be carried out before use in school and/or residential house is allowed.

It is important to note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Parental/carer support will be enlisted to minimise these risks.

Student mobile phones will not be used during lessons or formal school time. Exceptions to this can only be made by application to and the agreement of the Head of Site. The sending of abusive or inappropriate text messages or files by Electronic means is forbidden.

The use by young people of cameras in mobile phones will be kept under review.

Staff will be issued with a SENAD phone where contact with young people or adults is required or where mobile phones are used to capture photographs of young people/adults for evidence towards accreditation or achievement. **Personal phones must not be used to take photographs of students or make contact.**

Games machines including the Sony Playstation, Microsoft Xbox, Sky and BT Vision boxes and others which have internet access may not include filtering.

SENAD is under no obligation to provide internet connections for gaming devices – this will be subject to site internet facilities and connectivity. Games machines can download large amounts of data and where a site is on a limited capacity connection this data use may push the site over its allocated bandwidth. Care is required in any use in school or Home and an individual risk assessment should be undertaken.

Staff will monitor games played on these devices, for age appropriate (not all games have PEGI ratings), homophobic, racist, extreme language or sexual content, or some lifestyle web sites. Site/ Group guidelines may be used for unacceptable games.

The Group recognise the potential of tablets, hand held devices such as the iPod Touch, smartphones, smart watches as a learning platform, some of these devices are used within our schools to enhance the learning experience. The Group also encourage Students and Residents to use their own equipment. Staff and parents should be aware that some of these devices are capable of an independent data connection via mobile signal rather than site wireless and could be used to connect to the internet with no filtering where the data connection has been set up and paid for by a parent or guardian.

Should staff suspect that personal electronic devices have been used for internet misuse the Head of Site or Registered Manager should be informed. The photo or video content on the device should not be opened by the staff member reporting the issue.

Monitoring use of mobile devices by students is extremely difficult due to the ease with which the settings of the devices to allow private viewing of content access via the internet. Individual Risk Assessment, education/ training in safe use and limited monitoring by staff will be used as control measures. Sites may use loss of rewards or consequences systems to encourage safe use.

Parents that purchase electronic devices with paid internet access will be made aware that the device is capable of unfiltered content, and cannot be safely managed through the site filter systems. SENAD cannot accept responsibility for any content found on or consequences of the use of a device provided by parents with a third party data connection.

Individual sites may choose to confiscate the device if they suspect it is being used to download content that is illegal, age inappropriate,

or breaches the Local Acceptable Internet use guidelines. Return of the device will be discussed and agreed with the parents/guardian.

The E-safety coordinator will have a responsibility to continually update appropriate individuals in emerging technologies.

2.9 Offensive use of the Internet and the Law

Trolling

Trolling is a phenomenon that has swept across websites in recent years. Online forums, Facebook pages and newspaper comment forms are bombarded with insults, provocations or threats. Supporters argue it's about humour, mischief and freedom of speech. However, for many, the ferocity and personal nature of the abuse verges on hate speech. In its most extreme form it is a criminal offence.

"Online people feel anonymous and disinhibited," says Prof Mark Griffiths, director of the International Gaming Research Unit at Nottingham Trent University. "They lower their emotional guard and in the heat of the moment may troll either reactively or proactively, It is usually carried out by young adult males for amusement, boredom and revenge" he adds.

Arthur Cassidy, a social media psychologist, says young people's determination to create an online identity makes them vulnerable to trolling. Secrecy is jettisoned in favour of self-publicity on Facebook, opening the way for ridicule, jealousy and betrayal.

Trolling- The law

- The Communications Act 2003 governs the internet, email, mobile phone calls and text messaging
- Under section 127 of the act it is an offence to send messages that are "grossly offensive or of an indecent, obscene or menacing character"
- The offence occurs whether those targeted actually receive the message or not

2.10 Images contained on the young peoples personal devices:

Sexting:

Sexting has been identified as sending or receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging. If a student reports an incident of sexting to a staff member, staff are advised that viewing of the image could be either illegal or subject to a safeguarding concern. Staff should not under any circumstances attempt to investigate the content of a device themselves without the presence of other staff and discussion with the named person for Safeguarding.

Sexting incidents

If staff become aware of sexting by students, the device will be confiscated immediately and placed in a sealed container with the students' identity and a brief description of the incident. This container will be passed onto the Head of Site, Registered Manager or a member of the service's designated Safeguarding team. They will make the decision to either investigate further and/or seek advice through the Notify@senadgroup.com notification process. Staff are advised that it may be necessary to involve the police depending on the outcome of the investigation and whether illegal content is found. The document "'Sexting' in schools: advice and support around self-generated images" is available for reference and provides additional information on the correct handling of incidents.

2.11 Protecting personal data

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

3 Policy Decisions (Conduct)

3.1 Authorising Internet access

All staff must read the SENAD Computer, email and internet use company rules and guidelines.

Internet access provided by the sites will have an age appropriate filter. Schools with managed access will presume the parents or guardians of students accept the provision of a basic level of filtered access, within the boundaries outlined in this policy and local procedures/ Local Acceptable Internet use guidelines, unless they inform the schools otherwise. Sites may wish to involve parents on

an opt-in basis for provision of access to social networking, and access to internet facilities in residential areas.

Parents should be aware that while all care will be taken by SENAD to control internet access, due to the nature of wireless technologies there may be some areas of a site which have an unintentional overlap from approved usage areas – for example wireless coverage on a residential house sited over a classroom. Where this occurs staff should be vigilant for young people using the internet without supervision.

Any person not directly employed by the school shall not be allowed access to school ICT systems including the internet, unless agreed by a senior manager or a member of the IT team.

3.2 Assessing risks

The establishment will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the site network. The sites cannot accept liability for any material accessed, or any consequences of Internet access.

Mobile phones with wireless Internet access can bypass filtering systems and present a new route to undesirable material and communications. Parental/carer support will be enlisted to minimise these risks. For example to encourage the use of contracts with mobile operators that offer age sites filtering.

The establishment should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective.

All students and residents will be regularly risk assessed for E-Safety issues as part of the Risk Assessment Policy (217).

E-Safety risks checklist includes:

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites

- Bullying and threats (i.e."Cyber" bullying by email, mobile, Bluetooth etc.)
- Identity theft, impersonations
- Publishing inappropriate content
- Online gambling and purchasing
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

E-safety posters should be displayed as part of safeguarding

Age appropriate content

Potential issues must be raised with the e-Safety co-ordinator who will advise on additional control measures as necessary to minimise risks.

3.3 Handling E-safety complaints

Complaints of Internet misuse by students or resident will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Head of Site.

Complaints of a child/adult protection nature must be dealt with in accordance with site child/adult protection and safeguarding procedures.

Young people and parents will be informed of the complaints procedure (see SENAD Complaints Policy 714)

Young people, adults and parents (where relevant) will be informed of consequences for misusing the Internet.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues as required.

Staff are advised to refer to the Safeguarding Policies **506A (adults)** and **506C.1*** (children).**

4 Communications Policy

4.1 Introducing the E-safety policy to the individuals in our care.

E-Safety rules will be available in all rooms where computers are used and discussed with young people regularly.

Young people will be informed that network and Internet use will be monitored and appropriately followed up.

Training in e-Safety will be used for example the *Safe* programme of study in conjunction with the educational social network platform *Makewav.es* Additional materials may be developed, possibly based on the materials from CEOP.

E-Safety training will be embedded within the ICT scheme of work to help our young people become good safe and considerate users of the internet and emerging technologies.

4.2 Staff and the E-Safety policy

All staff will be trained in the SENAD E-Safety Policy and its importance explained. The Group will ensure all E-safety coordinators are kept up to date with changes to policy or dangers presented by emerging technologies.

4.3 Enlisting parents' and carers' support

Parents and carers attention will be drawn to the SENAD E-Safety Policy in newsletters, the school brochure and on the school Web site. The establishment will maintain a list of e-safety resources for parents/carers. Local procedures may be identified for access to the internet at the point of initial assessment.

4.4 Staff Training

As the strategic change from locked down to a managed system is introduced staff will have access to appropriate online safety training that is relevant to the young people and the staff that are responsible for managing access.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Young people should be supervised. Young people should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK
Using search engines to access information from a range of websites.	School Filtering must be active and checked frequently. Parental consent should be sought. Young people should be supervised whilst on school networks and managed whilst on Home networks. Young people should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick If Google – must be set to strict filtering and be supervised.
Exchanging information with other young people and asking questions of experts via email or blogs.	Young people should only use approved email accounts or blogs. Young people should never give out personal information. Consider using systems that provide	Makewav.es RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail

Activities	Key e-safety issues	Relevant websites
	online moderation e.g. SuperClubs Plus.	
Publishing young people' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Young people full names and other personal information should be omitted. Young people work should only be published on moderated sites and by the school administrator.	Makewav.es Making the News SuperClubs Plus Headline History National Education Network Gallery
Publishing images including photographs of young people in the public domain.	Not allowed.	
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be managed. Young people should never give out personal information.	Makewav.es SuperClubs Plus FlashMeeting

Activities	Key e-safety issues	Relevant websites
Audio and video conferencing to gather information and share young people' work.	Young people should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	Makewav.es FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

Safe

www.safesocialnetworking.org

www.radiowaves.co.uk (Makewav.es)

BBC Stay Safe

www.bbc.co.uk/cbbc/help/safesurfing/

Becta

http://schools.becta.org.uk/index.php?section=is

Chat Danger

www.chatdanger.com/

Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

Childnet

www.childnet-int.org/

Cyber Café

http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen

www.digizen.org/

Kent e-Safety Policy and Guidance, Posters etc

www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart

www.kidsmart.org.uk/

Kent Police – e-Safety

www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Think U Know

www.thinkuknow.co.uk/

Safer Children in the Digital World

www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents and adult service users

Care for the family

www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

http://publications.teachernet.gov.uk

Family Online Safe Institute

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk

Kent leaflet for parents: Children, ICT & e-Safety

www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre

www.parentscentre.gov.uk

Internet Safety Zone

www.internetsafetyzone.com

Appendix 4: Terms Used in this Policy and supporting documents

Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need
AUP	Acceptable Use Policy
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.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, and Nintendo DS. Also can include BT Vision, Sky and Virgin Media boxes.
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.

ICT	Information and Communications Technology or (ICT), is often used as an extended synonym for information technology (IT), but is a more specific term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as software, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.
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.
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 systems 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.
PEGI	Pan European Game Information (PEGI) is a European video game content rating system established to help European consumers make informed decisions on buying computer games with logos on games' boxes. It was developed by the Interactive Software Federation of Europe (ISFE) and came into use in April 2003; it replaced many national age rating systems with a single European system.
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 e-mails have links in them which take people to fake sites set up 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.
PSHE	PSHE education is a planned programme of learning through which children and young people acquire the knowledge, understanding and skills they need to manage their lives now and in the future
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SGII	Self-generated indecent images (often referred to as "sexting" –see above)
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 friends and stay in touch with people.
Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trolling	Inflammatory, extraneous, or off-topic messages in an online community such as a newsgroup, forum, chat room, or blog with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion.
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.