The SENAD Group

Section 5

Online Safety Policy

(E Safety)

Issue: September 2019
Reviewed: September 2019
Next Review: July 2020
Version: 8
Policy Ref: 510.0
Owners: BV

Online Safety (e-Safety) 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 Online 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.

This policy is informed by the non-statutory guidance from the Department for Education "Teaching Online Safety in school" published in June 2019. It is also informed by the "Education for a connected World" Framework, published by the UK council for Internet Safety.

The Head of Service will identify the online safety Co-ordinator for the SENAD site, who will liaise with the Designated Safeguarding Lead on online safety issues. Given the complementary role of both roles, the both roles could be carried out by the same person. The Head of Site/Registered Manager and online safety Co-ordinator will be responsible for defining the site/ Local Acceptable Internet use Guidelines.

This policy applies to SENAD 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 many 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 risks of Internet usage, yet allowing through a managed approach access to the Internet and its many possibilities.

The SENAD Group also recognises that young people with special educational needs are more likely to be victims of online abuse and harm, compared with young people without recognised SEN or disabilities; therefore systems, software and technologies will need to be approached with caution and continual monitoring.

It should be noted that due to the nature of the young people at some sites the general guidelines below may not always be appropriate (for example young people with inappropriate or with the potential to demonstrate illegal 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.

Principles:

- 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 online safety strategies
- Support 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.
- 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 Online safety which can be categorised into 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 to self or others.

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.

1 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**).

The teaching of safe use of the Internet and emerging technologies will be guided by the non-statutory guidance "Teaching online safety in school" (DFE, June 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf?_ga=2.153654392.1911543291.1566552075-1522255728.1551439363

and the "Education for a connected world framework" (UK Council for Internet Safety) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759003/Education_for_a_connected_world_PDF.PDF

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. In principle, all resident students and residents of adult facilities should be able to access the Internet as stated above. 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. Relevant programmes, activities and software will be used to teach this according to the age and ability of the young person. An example of relevant activities and guidance can be found in CEOP's initiatives for young people aged 5-18. 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 inappropriate and / or illegal Internet content as part of the PSHE and COMPUTING curriculum and how to use the school's Safeguarding Procedure. Staff will advocate on behalf of students who are unable to do this.

Adult service users will also be made aware of online safety and how to report illegal or harmful 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. Schools' and adult residential homes' filters will aim to exclude material and sites that promote hatred.

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 will be encouraged to 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.

Students will be taught to follow social interaction guidelines to interact online as they would do offline when contacting others via email or other online media (apps, social media) when using school and own devices. Students will be reminded and expected to put this in practice.

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 EU General Data Protection Regulation and Data Protection Act 2018 affects our use of photography. Written consent must be obtained from the student’s parent/guardian before taking photographs or making video recordings of students. Consent forms are available for this purpose. A student over the age of 13, whom is deemed to have capacity, must also agree with their parents/guardians consent for it to be valid as consent.

Consent for photography or video recording is sought when a young person is admitted and renewed annually. Parents/guardians 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 consent should have been obtained from the YP/parents as appropriate.

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 and school displays. 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 online safety coordinator and Registered Manager/Site Head.

The school might use an accepted educational platform for teaching digital citizenship and Online safety.

Online 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 and for young YP the advice will be to use only moderated social networking sites.

Young people and parents will be advised about the possibilities and risks the use of social network spaces. Staff are advised to refer to Policy **502** Anti bullying to deal with situations of online bullying.

Young people will be advised to use nicknames and avatars when using social networking sites and to follow social interaction guidelines as they would do when interacting offline.

Staff should refer to HR Policy **402** “Computer, Email and Internet Use” Policy when using social networks and in particular in regards to possible contact with current or ex-students/residents, and to comments placed on those 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 online 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 video chatting and live streaming

Where possible, video chatting, live streaming and any other 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. It is however possible that YP with access to their own mobile and with Internet access through their own network might bypass supervision if downloaded the app with their parents’ permission. Depending on the age of the young person, staff will contact parents at the earliest opportunity this has been noticed to verify they give permission for their child to engage in video chatting and / or live streaming.

Video conferencing and webcam use will be appropriately supervised for the pupil’s age, and level of understanding although this requires the co-operation of parents and YP particularly in the case of YP using their own mobile / device with own Internet access through a mobile network.

Where possible, 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). This needs to be balanced with the need to enable YP to video chat and live stream from areas where they can be easily supervised.

2.8 Managing emerging technologies

Emerging technologies will be, where necessary, examined for educational benefit and for concerning technologies, software and "apps" an individual risk assessment will be carried out before use in school and/or residential house is allowed. This risk assessment can be raised by any member of staff with the Senior Management team / Safeguarding team via the Safeguarding process for the site.

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 inappropriate material and communications. Parental/carer and YP's support and co-operation 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 (i.e. photos, videos, "memes") by Electronic means will be discouraged as school rule and dealt by through the appropriate policy (i.e. Anti-Bullying policy **502**)

Students and users will be educated on issues around use of cameras in mobile phones and electronic images. 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 or videos 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. YP will be advised to where possible use these devices for games within a supervised area, to behave online as they would do offline, and to report any concern to staff.

Staff will monitor with YP's co-operation games played on these devices, for age appropriateness (not all games have PEGI ratings), homophobic, racist, extreme, sexist or sexual language or content.. Site/ Group guidelines may be used for unacceptable games.

The Group recognise the potential of tablets and hand held devices such as the iPod Touch, smartphones and smart watches as a learning platform and 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 a separate data connection via mobile signal rather than site wireless connection 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. Parents will be enlisted to monitor frequently the content, contact or conduct engaged by their children on these devices, and supported to do so if parents feel they require this level of support. Staff will endeavour to provide as much supervision and dialogue in regards to this use as possible within the age and context of the YP. 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 a device if they suspect it is being used to download content that is illegal, age inappropriate, or breaches this policy guidelines Return of the device will be discussed and agreed with the parents/guardian (and / or the police if appropriate).

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

It is recommended that the Online Safety Co-ordinator for the site is also a CEOP Ambassador, having attended the training required for this, in order to have a good ground understanding of the issues faced. Continuous development through reading of safeguarding updates, Internet matters and other publications will nevertheless be required.

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.

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

  At SENAD

Staff in schools and homes will educate young people in the above legislation and discourage any attempts of trolling. Cases of trolling from or between students / residents will dealt by on an individual basis based on content, needs, ability, understanding and impact.

2.10 Images contained on the young people’s 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. However recent guidance (“Sexting in Schools and Colleges” from the UK Council of Internet Safety, UKCIS) explains that the most pertinent concern is the sending of explicit sexual images and videos by young people under the age of 18. This is defined as “youth produced sexual imagery” and is illegal to send, store, copy and forward both in paper copy and electronically. Nevertheless, it is also important to consider that the production of sexual imagery by vulnerable adults, although legal, can have devastating effects for the individual/s affected.

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 incident needs to be reported ASAP to a Senior Manager or staff following the site’s safeguarding procedure. They will make the decision on how either investigate further and/or seek advice through the notify@senadgroup.com notification process (see also policy **514**). 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 and colleges: responding to incidents and safeguarding young people” (UKCIS)” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759007/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf?_ga=2.153245048.1911543291.1566552075-1522255728.1551439363 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. However, please see paragraph 2.4 above for the pending changes to this legislation in May 2018.

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 unless they inform the schools otherwise.

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 access to Internet through personal data allowance can bypass filtering systems and present a new route to inappropriate material and communications. Parental/carer support will be enlisted to minimise these risks, such as encourage the use of contracts with mobile operators that offer age sites filtering.

The establishment should audit COMPUTING use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate and effective.

All students and residents will be regularly risk assessed for Online safety issues as part of the Risk Assessment Policy (**217**). The checklist of online risks YP should be assessed against will be based on the checklist provided by the "Teaching online safety in Schools" (DFE, June 2019) document https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf?_ga=2.149518582.1911543291.1566552075-1522255728.1551439363

Online safety posters should be displayed as part of safeguarding

Age appropriate content

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

3.3 Handling online 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.

Concerns 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)** Available on SharePoint

4 Communications Policy

4.1 Introducing the Online safety policy to the individuals in our care.

Online 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 Online safety will be used according to the age ability and need of the young people involved. Use of reputable resources such as NSPCC or CEOP websites will be guaranteed through quality Assurance of the Online Safety co-ordinator for the site. Online safety training will be embedded within the PSHE and Computing schemes of work to help our young people become good, safe and considerate users of the internet and emerging technologies.

4.2 Staff and the online safety policy

All staff will be trained in the SENAD Online safety Policy and its importance explained. The Group will ensure all online 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 Online safety Policy through newsletters, the school brochure and Senad SharePoint. The establishment will maintain a list of online 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

Staff 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:

List of areas to assess students' online risks (taken from the "Teaching online safety in school" (DfE. June 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf?_ga=2.149518582.1911543291.1566552075-1522255728.1551439363 (Also available on SharePoint)

- Age restrictions
- Digital footprint (including reputational damage)
- Sexting
- Understanding and acting on misleading information, hoaxes, "fake news"
- Fake websites, emails and profiles
- Online fraud
- Password phishing
- Sharing personal data
- Addiction and persuasion to remain online / purchase online
- Privacy settings
- Grooming and abuse
- Taking part in online challenges
- Incitement to hatred / violence
- Live Streaming
- Pornography
- Negative impact of online use on wellbeing (unrealistic profiles, photo manipulation, social pressure through chats, comments on websites etc.)
- Bullying and trolling (both as victim and perpetrator)