# The SENAD Group

## Section 5
## Online Safety Policy
(E-Safety in schools & children's homes)

**Also read the school's safeguarding policy**

Issue: November 2022
Reviewed: November 2022
Next Review: November 2023
Version: 12
Policy Ref: 510.0
Owners: MR

## Contents

# Online Safety (e-Safety) policy statement

The purpose of this policy is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

# How we keep children safe online

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and approach to online safety empowers the school and protects and educate students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. KCSIE 2022 and Welsh Government equivalent, groups the threats into four C's as follows:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The school will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures.

This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

We will take the following actions to achieve these goals:

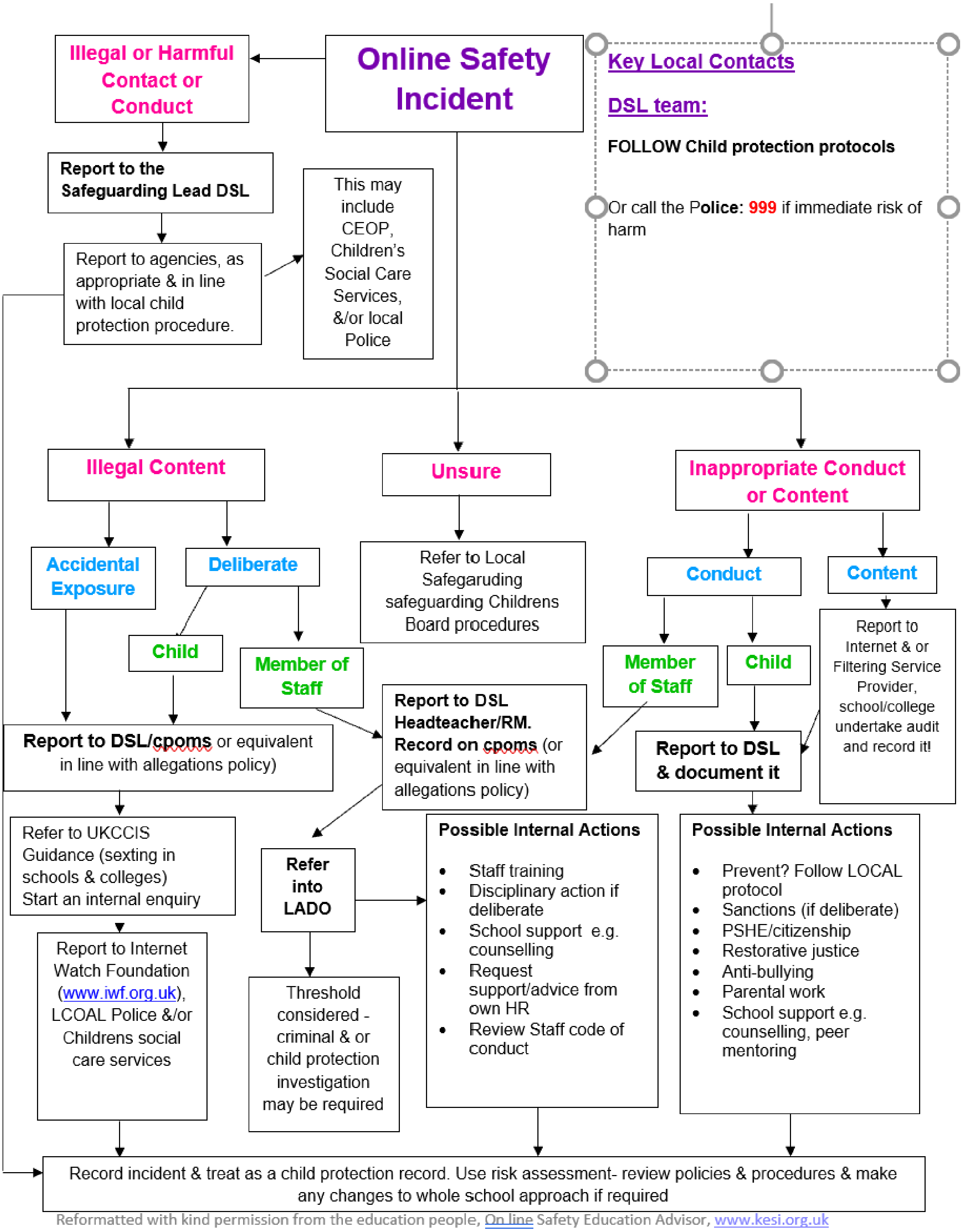
1. appoint an online safety coordinator and if they are not the lead DSL, this person will be actively supported by the DSL
2. providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
3. having appropriate filters, safety systems and control over devices
4. an approach to managing students who bring their own 4g/5g enabled devices
5. supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
6. supporting and encouraging parents and carers to do what they can to keep their children safe online
7. developing an online safety agreement for use with young people and their parents/carers
8. developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.

# How we respond to any abuse allegations

By having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)

- will follow the local safeguarding board's notification policies as set out in the school's safeguarding policy (which is available on the school's website).
- set out training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any other parties and our school as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

# Responding to an on-line safeguarding concern



Online Safety Incident

Illegal or Harmful Contact or Conduct

Report to the Safeguarding Lead DSL

Report to agencies, as appropriate & in line with local child protection procedure.

This may include CEOP, Children's Social Care Services, &/or local Police

Key Local Contacts

DSL team:

FOLLOW Child protection protocols

Or call the Police: 999 if immediate risk of harm

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL/cpoms or equivalent in line with allegations policy)

Refer to UKCCIS Guidance (sexting in schools & colleges)
Start an internal enquiry

Report to Internet Watch Foundation (www.iwf.org.uk), LCOAL Police &/or Childrens social care services

Unsure

Refer to Local Safegaruding safeguarding Childrens Board procedures

Report to DSL Headteacher/RM. Record on cpoms (or equivalent in line with allegations policy)

Refer into LADO

Threshold considered - criminal & or child protection investigation may be required

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate
- School support e.g. counselling
- Request support/advice from own HR
- Review Staff code of conduct

Inappropriate Conduct or Content

Conduct

Member of Staff

Child

Report to DSL & document it

Content

Report to Internet & or Filtering Service Provider, school/college undertake audit and record it!

Possible Internal Actions

- Prevent? Follow LOCAL protocol
- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School Support e.g. counselling, peer mentoring

Record incident & treat as a child protection record. Use risk assessment- review policies & procedures & make any changes to whole school approach if required

Reformatted with kind permission from the education people, On line Safety Education Advisor, www.kesi.org.uk

# Understanding harms and risks

Understanding and applying the knowledge and behaviours above will provide students with a solid foundation to navigate the online world in an effective and safe way. To do this, the school also needs an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their students.

Underpinning knowledge and behaviours include:

**How to evaluate what they see online -** This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Schools can help pupils consider questions including:

- is this website/URL/email fake? How can I tell?
- what does this cookie do and what information am I sharing?
- is this person who they say they are?
- why does someone want me to see this?
- why does someone want me to send this?
- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?

**How to recognise techniques used for persuasion** – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

Schools can help pupils to recognise:

- online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
- techniques that companies use to persuade people to buy something,
- ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and
- criminal activities such as grooming.

**Online behaviour** – This will enable pupils to understand what acceptable and unacceptable online behaviour look like. Schools should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

Schools can help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
- looking at how online emotions can be intensified resulting in mob[1] mentality,
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and
- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

**How to identify online risks** – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Schools can help pupils to identify and manage risk by:

- discussing the ways in which someone may put themselves at risk online,
- discussing risks posed by another person's online behaviour,
- discussing when risk taking can be positive and negative,
- discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

**How and when to seek support –** This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Schools can help pupils by:

- helping them to identify who trusted adults are,
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
- helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

[1] Mob mentality describes how people can be influenced by their peers to adopt certain behaviours on a largely emotional, rather than rational, basis

# 1 Teaching safe use of the internet

## 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.

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) and the "Education for a connected world framework" (UK Council for Internet Safety) Education for a Connected World (publishing.service.gov.uk)

**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 residential 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.

## 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**.**

## 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.

### 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 allow 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.

## 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/guardian's 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 site's 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 regard 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 reflected within school rules 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.**

**Game 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. Game 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 where we think it is safe to do so.

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/guardians** 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 young person.
- **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. **Neither the school nor 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 schools 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 or the Lead DSL 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.

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

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 Designated Safeguarding Lead.

### 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 how to 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)" Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) (December 2020) is available for reference and provides additional information on the correct handling of incidents.

## 2.11 Protecting personal data

The UK Data Protection Act 2018 and UK GDPR regulate the recording, storing and release of personal data. All students and users at SENAD locations will be taught about the implications for everyday use of the internet, including consent, confidentiality, use of encryption and passwords and other relevant aspects of the legislation.

## 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

**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 - using the child protection policy

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 protection nature must be dealt with in accordance with school's child protection and safeguarding procedures.

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

- Students' 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 Policy and **506C.1 (children)** which includes Part 1 of KCSIE 2022 Keeping children safe in education - GOV.UK (www.gov.uk)

## 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.

## Virtual lessons and live streaming

Remote teaching will include both recorded or live direct teaching time, and time for pupils and students to complete tasks and assignments independently. Online video lessons do not need to be recorded by teaching staff at the school or college: Oak National Academy lessons, for example, can be provided in lieu of school-led video content. Schools and colleges are best placed to decide on the most appropriate approach to teaching their pupils and students effectively.

If you choose to provide remote education using live streaming or pre-recorded videos, guidance from the National Cyber Security Centre (NCSC) on which video conference service is right for your school and using video conferencing services securely could help schools and colleges to set up video conferencing safely, specifically the section on deploying and configuring the service.

We know that some schools and colleges have concerns around live lessons, but if done correctly, we do not believe they pose additional safeguarding risks and can actually bring many benefits, including improved engagement. You may find the following useful when organising live lessons (this is not an exhaustive list):

- use neutral or plain backgrounds
- ensure appropriate privacy settings are in place
- ensure staff understand and know how to set up and apply controls relating to pupil and student interactions, including microphones and cameras
- set up lessons with password protection and ensure passwords are kept securely and not shared
- ensure all staff, pupils, students, parents and carers have a clear understanding of expectations around behaviour and participation

You may also find the following guidance useful:

- guidance from the UK Safer Internet Centre on safe remote learning which includes detailed advice on live, online teaching
- the safeguarding guidance from London grid for learning (LGfL) includes platform-specific advice
- The Key provides detailed advice including a sample risk assessment for planning live lessons
- SWGfL, using insight from the professional's helpline provides advice on cameras on or off and recording lessons

In some areas, schools or colleges may also be able to seek support from their local authority when planning online lessons and activities, and when considering online safety.

For Aran Hall School, the Welsh Government resources are also relevant:

https://hwb.gov.wales/zones/keeping-safe-online

## Safety plan for a student

A safety plan for a student who has a clear online risk, requires a risk assessment with an action plan for everyone to follow, including the school's staff, the student and the parent/guardians.

- Typically, the student should be involved in the plan
- Typically, the parent/guardian will be involved in the plan and also seek to follow it in their home.
- Shared with the student's social worker if residential student (irrespective of their legal status)

This plan should be kept under view, typically once a term, but more frequently if the student is at a higher risk.

## Risk analysis – factors to be considered

This section covers elements of online activity that could adversely affect a pupil's personal safety or the personal safety of others online. DfE external document template (publishing.service.gov.uk)

| Potential harm or risk | Description | Curriculum area this could be covered in |
|---|---|---|
| **Abuse (online)** | Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal.<br>Teaching could include<br>• explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation,<br>• explanation of when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail,<br>• how to respond to online abuse including how to access help and support,<br>• how to respond when the abuse is anonymous,<br>• discussing the potential implications of online abuse, including implications for victims,<br>• being clear what good online behaviours do and don't look like. | and how to report them."<br>Relationships Education core content (all stages) – online relationships. "about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help."<br>Relationship's education, relationships and sex education and health education – the law "Pupils should be made aware of the relevant legal provisions when relevant topics are being taught"<br>Health education core content (all stages) – internet safety and harms. "that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health"<br>Computing curriculum (all key stages) – "recognise acceptable/unacceptable behaviour; identify a range of ways to report |

| | | |
|---|---|---|
| | | concerns about content and contact.”<br>Citizenship: Key Stage 4 – Pupils should be taught about diverse national, regional, religious and ethnic identities in the United Kingdom and the need for mutual respect and understanding |
| **Challenges** | is and that while some will be fun and harmless, others may be dangerous and or even illegal,<br>• how to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why,<br>• explaining to pupils that it is ok to say no and not take part,<br>• how and where to go for help if worried about a challenge,<br>• understanding the importance of telling an adult about challenges which include threat or secrecy<br>• (‘chain letter’ style challenges). | Relationship’s education (all stages) and relationships and sex education (secondary) – “about online risks, including that any material someone provides to another has the potential to be shared online.”<br>Health Education core content (all stages) – “how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private”, “how to be a discerning consumer of information online” and “where and how to report concerns and get support with issues online.” |
| **Content which incites** | Knowing that violence can be incited online and escalate very quickly into offline violence.<br>Teaching could include:<br>• ensuring pupils know that online content (sometimes gang related) can glamorise the possession of weapons and drugs,<br>• explaining that to intentionally encourage or assist an offence is also a criminal offence,<br>• ensuring pupils know how and where to get help if worried about<br>involvement in violence. | Relationship’s education (all stages), relationships and sex education (secondary) and health education (all stages) – the law “Pupils should be made aware of the relevant legal provisions when relevant topics are being taught”. |
| **Fake profiles** | Not everyone online is who they say they are.<br>Teaching could include:<br>• explaining that in some cases | Relationship’s education core content (all stages) – online relationships. “that people sometimes behave differently online, including by pretending to be someone they are not.” |

| | | |
|---|---|---|
| | profiles may be people posing as someone they aren't (i.e. an adult posing as a child) or may be "bots" (which are automated software programs designed to create and control fake social media accounts),<br>• how to look out for fake profiles.<br>This could include<br>• profile pictures that don't like right, for example of a celebrity or object,<br>• accounts with no followers or thousands of follows; and<br>• Public figure who doesn't have a verified account | Computing curriculum (all stages) – "identify a range of ways to report concerns about content and contact." |
| **Grooming** | Knowing about the different types of grooming and motivations for it, for example radicalisation, Child Sexual Abuse and Exploitation (CSAE) and gangs (county lines).<br>Teaching could include:<br>• boundaries in friendships with peers and also in families and with others,<br>• key indicators of grooming behaviour,<br>• explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult; and<br>• how and where to report it both in school, for safeguarding and personal support, and to the police. Where there are concerns about sexual abuse and exploitation these can also be reported to Click CEOP.<br>See the NCA-CEOP Thinkuknow website for further information on keeping children safe from sexual abuse and exploitation.<br>At all stages, it will be important to balance teaching children about | Relationships Education (all stages) and Relationships and Sex Education (secondary) – "the characteristics of positive and healthy friendships (in all contexts, including online)". Relationships and Sex Education (secondary) includes, for example, "the concepts of, and laws relating to, sexual consent, sexual exploitation, abuse, grooming, coercion … and how these can affect current and future relationships" and "how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)." |

| | | |
|---|---|---|
| | making sensible decisions to stay safe whilst being clear it is never the fault of a child who is abused and why victim blaming is always wrong. | |
| **Live streaming** | Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children but it carries risk when carrying it out and watching it.<br>Teaching could include:<br>• explaining the risks of carrying out | Relationship's education core content (all stages) – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them"<br>Health education (secondary) |
| | live streaming. These include the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent. As such pupils should think carefully about who the audience might be and if they would be comfortable with whatever they are streaming being shared widely,<br>• online behaviours should mirror offline behaviours and considering any live stream in that context.<br>Pupils shouldn't feel pressured to do something online that they wouldn't do offline. Consider why in some cases people will do and say things online that they would never consider appropriate offline,<br>• explaining the risk of watching videos that are being live streamed, for example there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance,<br>• explaining the risk of grooming - see above for more on | core content – internet safety and harms. "the impact of viewing harmful content" |

| | | |
|---|---|---|
| | grooming. | |
| **Pornography** | Knowing that sexually explicit material presents a distorted picture of sexual behaviours.<br>Teaching could include:<br>• that pornography is not an accurate portrayal of adult sexual relationships,<br>• viewing pornography can lead to skewed beliefs about sex and in some circumstances can normalise violent sexual behaviour,<br>• that not all people featured in pornographic material are doing so willingly, i.e revenge porn or people trafficked into sex work. live streaming. These include the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent. As such pupils should think carefully about who the audience might be and if they would be comfortable with whatever they are streaming being shared widely,<br>• online behaviours should mirror offline behaviours and considering any live stream in that context.<br>Pupils shouldn't feel pressured to do something online that they wouldn't do offline. Consider why in some cases people will do and say things online that they would never consider appropriate offline, | RSE (secondary) core content – online and media. "that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners."<br>core content – internet safety and harms. "the impact of viewing harmful content" |

| | | |
|---|---|---|
| | - explaining the risk of watching videos that are being live streamed, for example there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance, explaining the risk of grooming – see above for more on grooming | |
| **Pornography** | Knowing that sexually explicit material presents a distorted picture of sexual behaviours.<br>Teaching could include:<br>- that pornography is not an accurate portrayal of adult sexual relationships,<br>- viewing pornography can lead to skewed beliefs about sex and in some circumstances can normalise violent sexual behaviour,<br>- that not all people featured in pornographic material are doing so willingly, i.e revenge porn or people trafficked into sex work. | Relationship & Sex Education (secondary) core content – online and media. "that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners." |
| **Unsafe communication** | Knowing different strategies for staying safe when communicating with others, especially people they do not know/have never met.<br>Teaching could include:<br>- explaining that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with,<br>- identifying indicators or risk and unsafe communications,<br>- identifying risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before, | Relationships education core content (all stages) – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them."<br>and "how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met."<br>Relationships Education core content (all stages) – respectful relationships. "the importance of permission-seeking and giving in relationships with friends, peers and adults"<br>RSE (secondary) core content – "the characteristics of positive and healthy |

| | | |
|---|---|---|
| | - explaining about consent online and supporting pupils to develop strategies to confidently say "no" to both friends and strangers online. | friendships (in all contexts, including online) including: trust, respect, honesty, kindness, generosity, boundaries, privacy, consent and the management of conflict, reconciliation and ending relationships. This includes different (non-sexual) types of relationship"<br>Computing curriculum (all key stages) – "identify a range of ways to report concerns about content and contact." |