Kent School of Veterinary Nursing

Online Safety Policy. Social Media Policy.

Created Feb 20 CG. Updated 1.4.21.CG Reviewed 3.9.21. CG

Scope of the Policy

This policy applies to all members of the *KSVN* community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school digital technology systems, both in and out of the school.

KSVN will deal with such incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within KSVN.

KSVN Directors

The KSVN Directors are responsible for the Online Safety Policy and for reviewing the effectiveness of the policy.

The Directors have a duty of care for ensuring the safety (including online safety) of members of the school community.

The Directors are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority / other relevant body disciplinary procedures).

The Directors :

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the KSVN online safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with appointed technical staff

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Updates are discussed at Directors meetings by Natalie as Safeguarding officer
- include online safety reports regularly at KSVN Team meetings

Network & iT Technical staff

The iT Technical Staff ensure

- that KSVNs technical infrastructure is secure and is not open to misuse or malicious attack
- that KSVN meets required online safety technical requirements.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that access & rights to networks, systems and applications is limited according to role (staff and students) & need and includes access at basic user& administrator/manager levels
- the filtering policy is applied if indicated and this is updated on a regular basis
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Safeguarding Officer for investigation / action / sanctions.
- that monitoring software / systems are implemented and updated as agreed in KSVN policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current KSVN Online Safety Policy and practices
- they report any suspected misuse or problem to the Director responsible for safeguarding for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies

- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- with the use of online video meetings for lessons (Zoom 2020 onwards due to Covid 19), that security is maintained regarding who has access to lessons. This includes access to video meetings via invite only with links sent direct to students. Attendees are held in a waiting room and admitted by tutor individually to ensure only those known are permitted to enter. All attendees have to log in by their recognised name (not nick name or device code) or will not be admitted to the session.
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Natalie Brudenell is the DSL and is trained in Online Safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Caroline George is the Deputy Designated Safeguarding Officer who support Natalie in her DSL role and provides DSL role in the absence of Natalie.

Online Safety monitoring – Safeguarding Director

Activities include:

- the production / review / monitoring of the KSVN Online Safety Policy / documents.
- reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs

- consulting stakeholders – including parents / carers /employers and the students / pupils about the online safety provision

Students

- are responsible for using the KSVN digital technology systems in accordance with the Student Use Agreement noted in the Course Handbook
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the KSVN Online Safety Policy covers their actions of site, if related to their membership of the school

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating student's to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of KSVNs online safety provision. Young people need the help and support of the KSVN team to recognise and avoid online safety risks and build their resilience.

Online safety should be present in all areas of the curriculum and staff should reinforce online safety message. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Online safety information is provided as part of Induction
- Key online safety messages should be reinforced as applicable in the classroom, especially when online research is particularly relevant / necessary.

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
  N.b. additional duties for education providers under the Counter Terrorism and Securities Act 2015 requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students should be helped to understand the need for safe and responsible use both within and outside KSVN.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Filters may be applied if necessary.

Education & Training – Staff

- A programme of online safety training / information update will be made available to staff. This will be regularly updated and reviewed at appraisal.

Technical – infrastructure / equipment, filtering and monitoring

KSVN will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

The KSVN technical systems will be managed in ways that ensure KSVN meets recommended technical requirements :

There will be regular reviews and audits of the safety and security of KSVN technical systems

Servers, wireless systems and cabling must be securely located and physical access restricted, where applicable

All users will have clearly defined access rights to KSVN technical systems and devices.

All users will be provided with a username and secure password. Users are responsible for the security of their username and password.

- Internet filtering / monitoring should be applied if considered a risk to ensure students are safe from terrorist and extremist material when accessing the internet.
- Personal data cannot be sent over the internet or taken off the KSVN site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising KSVNs wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in the KSVN context is educational. Use of mobile technologies is linked to the Safeguarding Policy, Behaviour Policy, Bullying Policy and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the KSVN Online Safety Induction sessions.

When using the KSVN laptops in class:

- These are allocated on a first come, first served basis and can only be reserved ahead in this system & via communication with the class tutor. There is currently one KSVN laptop available. Students are expected to usually have access to their own device.
- The laptops are available for KSVN course work use only and may not be removed from the training Centre nor used for personal use during the College day.
- Access to networks / internet is via the Centre wifi and of legal content & appropriate material only.

- Photographs may not be saved/downloaded. Passwords & screen backgrounds should not be changed.
- The installation of new apps, changing of settings or passwords is not permitted.
- Network / broadband capacity is linked to the strength of the setting from the Centre.
- Technical support is available in the first instance from the tutor/Centre staff who will then refer on to suitable iT support teams
- The KSVN laptops are not content filtered as students may be required to search for medical / animal terms, however if abuse of this becomes apparent, filters will be applied.
- Students can access course details from Onefile and information from the KSVN website.
- Students should not store any documents or personal records on the KSVN laptops, but email any work to themselves direct before deleting work from the laptop at the end of the college day.
- The laptops should not be removed from the classroom and not moved around the classroom without undue care.
- The tutor is responsible for monitoring the students use & handling of the laptop whilst in the classroom & ensuring its safe handling & storage after the class session.

Personal devices:

- Students (& tutors when appropriate) are allowed to use personal mobile devices in the class room when the tutor permits as part of planned or spontaneous classroom activity.
- Students may not use their personal devices in the classroom without tutor permission (See student contract)
- Students may charge their laptops and mobile phones using the safely secured electrical ports with tutor's permission.
- Staff are not allowed to use personal devices for KSVN business & should instead use the KSVN phones provided to individual staff to contact & message students etc. Staff phones can be used for taking college related photos of the students and scanning documents for storage in KSVN Dropbox etc with the images/documents then being deleted from the phone devices.
- Staff have access to networks / internet through the Centre's wifi and Onefile & the KSVN website etc.
- Network / broadband capacity is reliant on the wifi strength of the Centre (LAN router provided).
- Technical support is available from the Centre team in the first instance, or Natalie as the iT lead who may need to refer on as necessary.
- Staff KSVN laptops are not filtered for online use. The Data Protection Policy should be applied regarding the storage of student's personal details on the KSVN staff laptops / Dropbox site.

- If students are suspected of using their personal devices inappropriately the student may be interviewed by the tutor & the Student behaviour & Disciplinary Policy may be applied if necessary. The tutors reserve the right to check the student's personal device or report this to the Directors or other appropriate authority.
- Taking / storage / use of images or student personal documents on KSVN devices is permitted. Personal staff devices may not be used. KSVN laptops should not be used for personal private work.
- KSVN does not accept responsibility or liability for loss/damage or malfunction following access to the network or during use in the Centre/classroom with personal devices.
- Identification / labelling of personal devices is the responsibility of the owner. KSVN laptops are identified.
- Visitors are occasionally present at KSVN - sometimes for inspection purposes or as an external speaker. The CC team and TP Principals attend periodically. At times access to the Centre wifi is required. KSVN accept no responsibility or liability for loss/damage or malfunction following access to the network or during use in the Centre/classroom with personal devices.
- Information about the safe and responsible use of mobile devices is included in the KSVN Induction session.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils & employers need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers, Awarding Bodys & the Regulatory Body to carry out internet searches for information about potential and existing employees / student activities.

When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Permission from student (& parents where the student is <18yrs) is obtained before photographs of students / pupils are published on the KSVN website / social media / local press when

completing the Course Commitment Statement agreement and in the KSVN Student Contract. Any student not wishing to have their photograph taken should ensure they remind the tutor of this and remove themselves from the area.

- Students must not take, use, share, publish or distribute images of others without their permission. To do so without permission will be viewed as cyber bullying and the student behaviour / disciplinary process will be applied.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Where lessons are undertaken online with the use of video meetings (Zoom has been available & used since March 2020 due to Covid 19), most lessons are undertaken in muted/video off mode however for monitoring of the student for safeguarding purposes, it is important that at least when starting the video lesson, students are asked to have their video on, even just for a few minutes so the tutor has opportunity to visually check the safety of the learner. This would also give the learner opportunity to display a visual message of distress if needed.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

KSVN:

- has a Data Protection Policy
- is linked to the Information Commissioner's Office (ICO).
- Caroline George is the Director responsible for Data Protection. Natalie Brudenell is the Designated Safeguarding Lead, with Caroline the Deputy Safeguarding Officer.
- will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held is accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- Ensures a lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in the Privacy Policy.

- has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures are in place to deal with the individual rights of the data subject via student request to see all or a part of their personal data held by the data controller – see Data Protection Policy.
- There are clear and understood data retention policies and routines for the deletion and disposal of data. – see Data Protection Policy.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities at staff induction & at annual appraisal.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices/systems.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected or the information moved so that it can be.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with data protection policy once it has been transferred or its use is complete.
  Examples may include documents scanned onto the staff work phone, images of the student e.g. ID card or during class activities.

Communications

KSVN will communicate with students & TP staff via email, text messages, the website and occasionally Whatsapp as well as its Facebook page, Instagram site and twitter account.

- (The email service provided to KSVN students via its sub-contracting partners (N Kent / Hadlow College, may be regarded as safe and secure and is monitored. Users should be aware that these communications may be monitored.)
- Users must immediately report to their tutor, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official KSVN systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information will not be posted on the KSVN website and only official email addresses should be used to identify members of staff.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the concerns should be reported to the Data Protection Officer / Safeguarding Officer.

Other Incidents

It is hoped that all members of the KSVN community will be responsible users of digital technologies, who understand and follow Policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the KSVN team will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority, sub-contractor agent or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the KSVN DPO and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

KSVN Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school team are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

KSVN SOCIAL MEDIA POLICY

For the purposes of this policy, social media shall include but not be exclusive to Facebook, Instagram, Twitter, TikTok, YouTube, Wikipedia & Pinterest.

KSVN uses some forms of social media for general marketing purposes, as a promotional tool and to communicate to stakeholders. Staff & students are encouraged to use IT, including social media to research, communicate and engage with the global veterinary profession. However, when doing so particular attention should be given to the KSVN policies of Equality, Diversity & Inclusion; Confidentiality; Anti-bullying & Anti-harassment; Safeguarding and Online Safety Policies, which apply to all forms of communication including social media both inside & outside of the work environment.

STAFF USE OF SOCIAL MEDIA

As members of the KSVN team, employees have a responsibility to not damage the KSVN reputation or ethos of high standards. The KSVN Directors reserve the right to monitor employee use of social media to ensure it is appropriate in respects to comments made on, but not limited to employees; students; Training Practices and other stakeholders.

When the KSVN team use social media to positively share information & provide support the following should be borne in mind:

- Apply sensible behavioural standards – not saying anything online that you wouldn't say in person.
- To not engage in social media activities, forums or confrontations that may bring KSVN into disrepute.
- Never engage in harmful, threatening or defaming conduct to others.
- Consider carefully any addition or comment on forums or conversations & if considered appropriate to do so, ensure it is clear that you are doing so independent of your place of

employment and the details you provide are not representative of your place of work. You should not mention your place of work or display any details that include this. You must take full responsibility for any information you add, exercising good judgement & common sense. The carefully written comments should include the following statement "the views expressed above are my personal views alone and should not be interpreted as the official policy or opinion of my place of employment".

- Only those who have received express permission from the Directors can contribute in the name of KSVN & only then with express permission, may KSVN logo's or other business details be used. Account details, user names and passwords for these accounts should be passed on to one of the Directors. One of the Directors should be included in the group message for monitoring purposes and continuity should the original staff contributor leave.
- Be mindful of any conflicts of interest.
- Never disclose confidential or non-public information about KSVN and should bear in mind Data Protection Act and GDPR, avoiding divulging personal details about themselves, colleagues, students or stakeholders.
- Only staff work phones may contain contact details for students, TP staff or other stakeholders. Any groups – official or unofficial e.g. whatsapp groups or Facebook groups may only be created on these phones and only with express permission of the Directors. Monitoring of these groups, when administered by the individual staff member, remains the responsibility of the staff member.

Failure to abide by the above statements could result in disciplinary action being taken.

Social media channels are monitored regularly so that any comments relating to KSVN may be acted upon. If team members discover negative or erroneous statements concerning KSVN on social media sites, you should only respond if you have appropriate knowledge and the permission of the Directors. All comments discovered should be forwarded to the Directors.

STUDENT USE OF SOCIAL MEDIA

KSVN respect the right of freedom of speech for all students as one of the British Values, however the protect the reputation of KSVN students:

- Apply sensible behavioural standards – not saying anything online that you wouldn't say in person.
- Not engage in social media activities, forums or confrontations that may bring KSVN into disrepute.

- Never engage in harmful, threatening or defaming conduct to others.
- To not add any information under the pretext of it being KSVN content or opinion. They must not infer the information is supported by anyone from the KSVN team, but instead take responsibility themselves.
- Not use any KSVN imagery or logos unless prior written agreement has been obtained from one of the Directors.
- If mention is directly made of KSVN, that this does not bring KSVN or it activities or staff into disrepute.
- Be aware of KSVN's social media related policies including: Equality, Diversity & Inclusion; Confidentiality; Anti-bullying & Anti-harassment; Safeguarding and Online Safety Policies.
- Not add any assessment information online be it queries, versions of questions for support nor complaints and issues. This applies to Centre based assessments by KSVN or Awarding Organisation assessments (external exams).

GOOD PRACTICE GUIDELINES FOR SOCIAL MEDIA

Be authentic Your presence on social media should, to some extent, be an extension of yourself. Conduct yourself professionally online and you will not go far wrong.

Consider your audience Remember that your potential readers could include current friends and possibly future employers. Therefore do not do anything to alienate these groups which you may live to regret – the internet does not forget and the VN profession is a very small, close world.

Be responsive Always seek the correct answers to questions posed and respond quickly.

Add value Although some people may be interested in life's trivia, the time you spend on social media will pay dividends if you add value to your fans, followers or readers. You need to be constructive. Let your fans, followers and readers know of an interesting article, or video which you've found, or give them tips on your area of expertise.

Respect copyrights and fair use This is obvious – always give people proper credit for their work and make sure you have the right to use something before you publish. This leads back into authenticity and integrity, never attempt to pass something off as your own which isn't.

Act according to the social media site you're on - what you post on Facebook and YouTube should be different to what is included on LinkedIn or blogs which relate to your area of expertise. Understand the network and act accordingly.

Don't forget your personal security Don't give out your email address, telephone number or bank details etc. Even giving your full name should be avoided and log in names should not include birthday/DoB information. Ensure you take care of your personal data and safety.

Don't overreach yourself There is nothing worse than developing an online audience only to find that you cannot deliver. When entering the online environment you must remember that there are other important thing in life such as family, work, your studies and friends. These should be your priority first.

Realise that perception is reality In the online world the lines between public and private, personal and professional are blurred. Just by identifying yourself as a KSVN employee or student could create perceptions about your expertise, and about KSVN, by our numerous external stakeholders as well as the general public. Therefore be sure that all content associated with you is consistent with your work, the values of KSVN values and any professional standards. Check the Social Media Policy before you add reference to KSVN.

Be honest If you make a mistake, admit it. If you are modifying an earlier post then be transparent and explain why you are modifying it.

Pause for thought In social media it is all too easy to hit 'enter' and consider the consequences afterwards. However, before you commit yourself, re-read and check that you're comfortable with the message and the way it has been constructed. If you're unsure, re-word it until you're happy and then get the advice from a third party. You are responsible for what you publish, so be sure.

Address the basics With spelling and grammar checkers commonplace there is now no excuse for poor English. You will be judged by what people see so, to appear professional, ensure your posts have the correct punctuation and spellings.

Take all negative conversation off line as soon as you can. You must be responsive to criticism and negative comment but never engage in arguments online