

## KSVN Data Protection Policy

KSVN is required to keep certain information about employees, students, Clinical Coaches & employers and other users to allow it to monitor performance, achievements, health and safety, recruitment etc.

KSVN also has legal obligations to submit data to government funding bodies / agencies. To comply with the law, information must be used fairly, stored safely and not be disclosed to any person unlawfully. The ICO has determined KSVN does not need a Data Protection Officer.

## Data Protection Principles

To do this, KSVN must comply with the Data Protection Principles which are set out in the General Data Protection Regulations 2016 (GDPR). In summary these state that personal data shall:

*Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;*

*Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;*

*Be adequate, relevant and not excessive for those purposes;*

*Be accurate and kept up to date;*

*Not be kept for longer than is necessary for that purpose;*

*Be processed in accordance with the data subject's rights;*

*Be kept safe from unauthorised access, accidental loss or destruction; (see password policy section)*

*Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data;*

All KSVN staff who process or use any personal information must ensure that they follow these principles at all times.

KSVN is registered with the Information Commissioners Office & is bound by their regulations. The Director responsible for data protection compliance is Caroline George.

## Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by KSVN from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with one of the Directors initially. If the matter is not resolved it should be raised as a formal grievance.

## Notification of Data Held and Processed

All staff, students and other users are entitled to:

*Know what information KSVN holds and processes about them and why.*

*Know how to gain access to it.*

*Know how to keep it up to date.*

*Know what KSVN is doing to comply with its obligations under GDPR.*

KSVN will update staff data at least annually. Students' data is updated annually through the enrolment process.

## Responsibilities of Staff

*To check that any information that they provide to KSVN in connection with their employment is accurate and up to date.*

*To inform the KSVN of any changes to information, which they have provided. i.e. changes of address.*

*Checking the information that the KSVN will send out from time to time, giving details of information kept and processed about staff.*

*To inform KSVN of any errors or changes. KSVN cannot be held responsible for any errors that have not been notified.*

If and when, as part of their responsibilities, staff collect information about other people, (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.

## Data Security

All staff are responsible for ensuring that:

*Any personal data which they hold is kept securely.*

*Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.*

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information should be

*kept in a locked filing cabinet either on the KSVN premises or in a Directors home office or*

*if it is computerised, be password protected on the computer or virtual storage; or stored only on USB which is itself secure.*

### **Information Management Processes**

*Where electronic documents containing personal details are to be sent to others electronically, these will be sent using secure systems, protected with password only access.*

Data records (paper or USB) can only be taken from the premises subject to approval from one of the Directors. This could include, but not be limited to:

*Backup USB of Student Data – stored externally*

*Critical incident File – stored externally*

*Data stored on personal laptop computers, used externally to KSVN premises*

*Personnel Data stored externally for the purposes of emergency contact or Health and Safety*

### **Data Password protection information**

Staff are required to apply password protections to their devices – this includes work phones and laptops. This is to limit access to our systems which includes data about the team and the students.

To access the Microsoft 365 system and cloud storage on devices, KSVN team are required to use the Microsoft Authenticator app when using a device for the first time or whenever periodically prompted.

Passwords are used for general access on a trusted device with a timed cut off applied if the device is dormant for +15 minutes. The device should be set up to be re-activated with use of a PIN code or password.

Passwords must be specific to the device and not used elsewhere. They should contain at least 8 characters and include lower & upper case letters, digits and special characters. These should not be easily guessed words or names.

For other systems two step verification is used, linked to work phone numbers or emails. Windows Hello is available on KSVN devices to assist with this.

<https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>

### **Student Obligations**

Students must ensure that all personal data provided to KSVN is accurate and up to date. They must ensure that changes of address, etc are notified to the tutor or QV via email as appropriate.

### **Rights to Access Information**

Staff, students and other users of KSVN have the right to access any personal data that is being kept about them either on computer or in certain files.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing to one of the Directors.

Created Oct 19 CG. Annual review due each August. Reviewed 15 Aug 20 CG. Reviewed 3.9.21. CG. Reviewed 28.9.22 CG & edited (passwords) 16.11.22. reviewed 24.9.23. CG

Any person who wishes to subsequently exercise this right should complete a written request and forward it to one of the Directors.

KSVN will make no charge for the first occasion that access is requested, but may make a small administration charge for each subsequent request at its discretion.

KSVN aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

### Subject Consent

In many cases, KSVN can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to KSVN processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions. This is included as part of the recruitment process and is included on every student's individual learning agreement.

KSVN will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma, life threatening allergies or diabetes. KSVN will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

### Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure KSVN is a safe place for everyone, or to operate other KSVN policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for KSVN to do this.

Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Directors.

### Examination Marks

Students will be entitled to information about their marks for both internal & external assessments and examinations. However, this may take longer than other information to provide. KSVN may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the school.

### Retention of Data

KSVN will keep some forms of information for longer than others. Because of data retention legislation, information about students will not be kept indefinitely, unless there are specific requests to do so. The RCVS require student & TP records to be kept for five years, post qualifying/completing/leaving the course/ ceasing to be a TP.

Created Oct 19 CG. Annual review due each August. Reviewed 15 Aug 20 CG. Reviewed 3.9.21. CG. Reviewed 28.9.22 CG & edited (passwords) 16.11.22. reviewed 24.9.23. CG

## Disposal of Data

When personal data is no longer required or has passed its retention date, paper records will be shredded.

Computerised records will be permanently deleted, with particular care taken that 'hidden' data cannot be recovered.

## Compliance

Compliance with GDPR is the responsibility of all members of the KSVN team. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to KSVN facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with one of the Directors. Any breached in this Policy will be reported to the ICO within 72 hours of its presentation, as far as possible.

## Student Confidentiality Policy

This Policy is closely linked to the Data Protection Policy and includes information on the following:

Background to confidentiality and the Purpose of Policy, Safeguarding, Need to Know Basis, Parental Responsibility, Confidentiality, Counselling, Access to Personal Data by Learners, Behaviour and Disciplinary Issues, Learners with Disabilities and/or Learning Difficulties, Consent.

## Breaches in Data protection

Any breaches in data protection must be reported to the Data Protection Officer immediately, both verbally & in writing. A log will then be made with suitable responses made according to external guidance and a report being sent to the Information Commissioners Office, within 72 hours of the breach.

## Appendix

### Staff Guidelines for Data Protection (Including Safeguarding)

#### *Types of Data*

All staff will process data about students on a regular basis, when marking registers, or work, writing reports or references, or as part of a pastoral or academic supervisory role.

KSVN will ensure that all students give their consent to this sort of processing. This is completed during enrolment. Ethnicity or race, gender, age and information on learning difficulties and/or disabilities are also collected at enrolment. This information is sensitive and can only be collected and processed with the student's consent, which is included in the enrolment process.

The information that staff deal with on day-to-day basis will be 'standard' and will cover categories such as:

General personal details such as name and address, details about class attendance, course work marks and grades and associated comments. Notes of personal supervision, including matters about behaviour discipline, or information gathered at a tutorial session

Non standard information which may also be collected may include information about a student's physical or mental health; sexual life; political or religious views; trade union membership.

Examples : recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of personal duties.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the KSVN Data Protection Policy.

In particular, staff must ensure that records are:

accurate; up-to-date; fair; stored and disposed of safely, and in accordance with the KSVN policy.

KSVN designate all staff as 'authorised staff', meaning that staff are authorised to hold or process data that are deemed sensitive, or non standard.

### **Safeguarding & Data Protection**

Under safeguarding, the local authority has the legal duty to investigate situations where there is a risk of "significant harm".

All staff at KSVN have the responsibility to report concerns or disclosure of abuse, to the Directors for reporting to the local authority.

Learners have a right to confidentiality and privacy which must be respected. All communication about the case must be kept to a minimum on a "needs to know" basis. Where possible, the name of the individual learner should not be used.

KSVN staff cannot promise confidentiality and this must be made very clear to the learner when a disclosure is made. Learners must be told what will happen to them when a disclosure is made to a member of staff.

Authorised staff will be responsible for ensuring that all data is kept securely.

Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from one of the Directors, or in line with the KSVN policy. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the Directors, or in line with KSVN policy.

Before processing any personal data, all staff should consider the following checklist.

#### *Staff Checklist for Recording Data*

1. Do you really need to record the information?
2. Is the information 'standard' or is it 'sensitive'?
3. If it is sensitive, do you have the data subject's express consent?
4. Has the student been told that this type of data will be processed?
5. Are you authorised to collect/store/process the data?
6. If yes, have you checked with the data subject that the data is accurate?
7. Are you sure that the data is secure?
8. If you do not have the data subject's consent to process, are you satisfied it is in the best interests of the student or the staff member to collect and retain the data?
9. Have you reported the fact of data collection to the authorised person within the required time?

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf)