Policy: Data Protection and Freedom of Information

Member of Staff Responsible: **Alison Hesley**

Policy Approved By: **SCITT Strategic Board**

Approved on: **28.02.2017**

Review Date: **2020**

(circumstances may require an earlier review)

Signed-off by: **Strategic Board Chair:** _____

Andrew Cummings

Date: **04.07.2017**

Red Kite Teacher Training
DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

This document is a statement of the aims and principles of the Red Kite Teacher Training, for ensuring the confidentiality of sensitive information relating to staff, trainees, applicants to the SCITT and other users (tutors, trainers, and the management board).

Introduction

Red Kite Teacher Training needs to keep certain information about its staff, trainees and other users to allow it to monitor performance, achievements, and health and safety.

It is also necessary to process and store information relating to personal identification which may include for example names, contact details, academic achievements and progress.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Red Kite Teacher Training must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

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 that purpose.
- 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.

Red Kite Teacher Training and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the SCITT has developed this Data Protection Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, or the Contract for Trainees but it is a condition that employees and trainees will abide by the rules and policies made by the SCITT. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

The SCITT as a body corporate is the Data Controller under the 1998 Act, and the Strategic Board are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The SCITT has four Designated Data Controllers: They are the SCITT Director, the SCITT Senior Administer and two SCITT Administrator.

Any member of staff, trainee or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with the appropriate Designated Data Controller, who would be the SCITT Director.

Responsibilities of SCITT Users

All users and trainees are responsible for:

- Informing the SCITT of any changes to information that they have provided, e.g. change of address. The SCITT cannot be held responsible for any errors unless the user or trainee has informed the SCITT of such changes.

If and when, as part of their responsibilities, staff or users collect information about other people (e.g. about a trainee's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines in the SCITTs Data Protection Code of Practice as set out in Appendix A.

Data Security

All users (including trainees) are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

All users and trainees 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, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a memory stick or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe when not in use.

Data Protection Code of Practice

This code of practice is an appendix to the Data Protection Policy and offers specific guidance for staff, trainees and other users in relation to Data Protection at RKTT. This Code of Practice should be read alongside the Data Protection Policy. Specific practical guidance for Data Controllers and other users includes ensuring that;

- Personal information is kept in a locked filing cabinet /drawer with the key removed and stored in a secure place when not being used.
- Personal information is not left unattended.
- Computers, memory sticks and other removable media are coded/encrypted or password protected and secured when not in use.
- Data is processed in accordance with the Data Protection Policy
- Trainees and other users are made aware of the guidance within this policy
- Information on unsuccessful applicants is destroyed within 6 months of the start date of the course for which they applied.
- Personal files relating to trainees will be kept for 6 years. Following this a summary sheet including last known contact details and final grade will be kept as a record of course completion

Specific practical guidance for trainees includes ensuring that;

- They have understood and signed the Trainee Course Contract agreeing that they will adhere to guidance on specific Policies or Agreements such as Data Protection/ Use of Electronic Media etc
- They do not refer to pupils by name in training records, whether written or computerised, to protect their identity

Rights to Access Information

All staff, trainees and other users are entitled to:

- Know what information the SCITT holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the SCITT is doing to comply with its obligations under the 1998 Act.

This Policy document and the SCITT's Data Protection Code of Practice address in particular the last three points above.

To address the first point, the SCITT will, upon request, provide all users and trainees with a statement regarding the personal data held about them. This will state all the types of data the SCITT holds and processes about them, and the reasons for which they are processed (Appendix B)

All users and trainees have a right under the 1998 Act to access certain personal data being kept about them either on computer or in certain files.

Any person who wishes to exercise this right should express this in writing to the Designated Data Controller.

The SCITT will make a charge of £10 on each occasion that access is requested, although the SCITT has discretion to waive this.

The SCITT aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent

In many cases, the SCITT can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained.

Agreement to the SCITT processing some specified classes of personal data is a condition of acceptance on the course for trainees. This includes information about previous criminal convictions.

The SCITT course will bring trainees into contact with children. The SCITT has a duty under the Children Act 1989 and other enactments to ensure that trainees are suitable for their role.

The SCITT may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The SCITT will only use this information in the protection of the health and safety of the

individual, but will need consent to process this data 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, or race. Because this information may be considered **sensitive** under the 1998 Act, trainees and users will be asked to give their express consent for the SCITT to process this data. An offer of a place on the SCITT course may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to SCITT staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the SCITT.

Retention of Data

The SCITT has a duty to retain some staff and trainee personal data for a period of time following their departure from the SCITT, for purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the SCITT. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Date: July 2016
Review: