# Suffolk and Norfolk SCITT Data Protection Policy

## Introduction

Suffolk and Norfolk SCITT is committed to being transparent about how it collects and uses the personal data of its trainees, employees, consultants, mentors, contractors, partner schools and partner organisations and to meeting its data protection obligations.

This policy sets out Suffolk and Norfolk SCITT's commitment to data protection, and individual rights and obligations in relation to personal data.

Suffolk and Norfolk SCITT has appointed Sian Durrant of School's Choice as its data protection officer. Her role is to inform and advise the organisation on its data protection obligations. She can be contacted at data.protection@schoolschoice.org and questions about this policy, or requests for further information, should be directed to her.

## Definitions

- Personal data – any information that relates to an individual who can be identified from that information.
- Processing – any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
- Special categories of personal data – means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
- Criminal records data – means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

## Data Protection Principles

Suffolk and Norfolk SCITT processes personal data in accordance with the following data protection principles:

- Suffolk and Norfolk SCITT processes personal data lawfully, fairly and in a transparent manner.
- Suffolk and Norfolk SCITT collects personal data only for specified, explicit and legitimate purposes.
- Suffolk and Norfolk SCITT processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Suffolk and Norfolk SCITT keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Suffolk and Norfolk SCITT keeps personal data only for the period necessary for processing.
- Suffolk and Norfolk SCITT adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- Suffolk and Norfolk SCITT tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where Suffolk and Norfolk SCITT processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the General Data Protection Regulation (GDPR).

Suffolk and Norfolk SCITT will update personal data promptly if an individual advises that their information has changed or is inaccurate. Data gathered is held in:

- Trainee personal and progress files (in hard copy or electronic format, or both)
- Unsuccessful applicants' recruitment and selection paperwork (in hard copy or electronic format, or both)
- Employees and consultants files (in hard copy or electronic format, or both)
- On Suffolk County Council's and Norfolk County Council's HR systems

The periods for which Suffolk and Norfolk SCITT holds personal data are contained in its privacy notices/retention schedule. The organisation keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

## Data Retention

Suffolk and Norfolk SCITT maintains a retention schedule which is based on guidance from the information and records management society: http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school

We will only retain personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Data on unsuccessful applicants to our courses (paper and electronic) will be kept for 1 academic year and then destroyed.

Data on trainees (paper and electronic) will be kept for 7 years after training is completed and will then be destroyed.

We will keep a record of the personal email addresses of NQT so that we can stay in contact to offer support after the course is complete.

## Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

### Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, Suffolk and Norfolk SCITT will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;

- their right to complain to the Information Commissioner if they think the Suffolk and Norfolk SCITT has failed to comply with their data protection rights.

Suffolk and Norfolk SCITT will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should complete the relevant form/send the request to anna.richards@suffolk.gov.uk. In some cases, the Suffolk and Norfolk SCITT may need to ask for proof of identification before the request can be processed.

Suffolk and Norfolk SCITT will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Suffolk and Norfolk SCITT processes large amounts of the individual's data, it may respond within three months of the date the request is received. Suffolk and Norfolk SCITT will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, Suffolk and Norfolk SCITT is not obliged to comply with it. Alternatively, Suffolk and Norfolk SCITT can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which Suffolk and Norfolk SCITT has already responded. If an individual submits a request that is unfounded or excessive, Suffolk and Norfolk SCITT will notify them that this is the case and whether it will respond to it.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require Suffolk and Norfolk SCITT to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override Suffolk and Norfolk SCITTs legitimate grounds for processing data (where the Suffolk and Norfolk SCITT relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override Suffolk and Norfolk SCITT's legitimate grounds for processing data.

To ask Suffolk and Norfolk SCITT to take any of these steps, the individual should send the request to anna.richards@suffolk.gov.uk.

## Freedom of Information

Suffolk and Norfolk SCITT is subject to The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) and all requests for information that is not personal information must be treated as a FOI or EIR. These requests must be fully responded within 20 working days by law. The information will be provided unless Suffolk and Norfolk SCITT can provide an exemption or exception under the FOI act or EIR respectively.

## Data Security

Suffolk and Norfolk SCITT takes the security of personal data seriously. It has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or

disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Suffolk and Norfolk SCITT is working towards a clear desk policy.

Where Suffolk and Norfolk SCITT engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

An Information Risk Register will be created and maintained by Suffolk and Norfolk SCITT which summarises each information asset the organisation maintains. Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned.

**Data Breaches**

If Suffolk and Norfolk SCITT discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Suffolk and Norfolk SCITT will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**Individual Responsibilities**

Individuals are responsible for helping Suffolk and Norfolk SCITT keep their personal data up to date. Individuals should let Suffolk and Norfolk SCITT know if data provided to the organisation changes, for example if an individual moves house.

Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, Suffolk and Norfolk SCITT relies on individuals to help meet its data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

**Training**

Suffolk and Norfolk SCITT will provide training to all individuals (including trainees and consultants) about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

**Suffolk and Norfolk SCITT Staff**

- All staff sign the Suffolk and Norfolk SCITT Privacy Statement and have an annual data protection briefing.
- All staff have received a copy of the Suffolk and Norfolk SCITT Data Protection Policy and sign to say they have read and understood it.
- Suffolk and Norfolk SCITT staff will keep data on trainees on G Suite or the relevant Suffolk or Norfolk County Council networks which are fully secure.

**Trainees**

- All trainees sign the Suffolk and Norfolk SCITT Privacy Statement and agree that their information can be shared with Suffolk and Norfolk SCITT staff, consultants, staff in partnership schools and the University of Suffolk where it is necessary in order for us to fulfil the training contract that we have entered into with them.
- All trainees have a GDPR briefing session prior to coming into school so they understand the importance of data protection. They understand that they must know and act on each school's own data protection policy.
- All trainees receive a copy of the Suffolk and Norfolk SCITT Data Protection Policy and sign to say they have read and understood it
- All trainees use their Suffolk and Norfolk SCITT email addresses for any communication relating to the course.
- Suffolk and Norfolk SCITT trainees use G Suite as a secure cloud-based data storage solution for information relating to the course. Trainees will upload all course information containing any pupil related information or data (including lesson observations, weekly reflections etc) to the relevant secure G Suite areas and not keep any such information locally on their own devices.
- Trainees may keep some course information (e.g. lesson plans) in paper based files where this is acceptable under each schools' data protection policy. Information will be anonymised as far as is possible.

**NQTs**

- Unless consent is withdrawn, Suffolk and Norfolk SCITT will retain details of NQT personal email addresses to enable on-going support and contact.

**Suffolk and Norfolk SCITT Consultants**

- All consultants sign the Suffolk and Norfolk SCITT Privacy Statement and have an annual data protection briefing.
- All consultants receive a copy of the Suffolk and Norfolk SCITT Data Protection Policy and sign to say they have read and understood it.
- All consultants will use their Norfolk SCITT email addresses for any communication relating to the course.
- Consultants will use G Suite as a secure cloud-based data storage solution for information relating to the course. They upload all course information containing any pupil related information or data (including lesson observations, weekly reflections etc) to the relevant secure G Suite areas and not keep any such information locally on their own devices.

## Roles and Responsibilities

The senior information risk owner (SIRO) for the Suffolk and Norfolk SCITT is Anna Richards

They are responsible for:

- Owning and updating this policy
- Owning the risk register
- Advocating information risk management and raising awareness of information security issues

**All staff are responsible for ensuring that information is managed according to this policy.**

## Policy Review

Anna Richards, Executive Leader, and Sian Durrant, Data Protection Officer, are responsible for monitoring the arrangements set out in this document.

The policy will be reviewed every 2 years.

Written and agreed: May 2018

Updated: August 2018

Reviewed: May 2020

Next Review: August 2021