THE SOLENT SCITT GDPR PROTOCOLS

The General Data Protection Regulation (GDPR) comes into effect on 25th May 2018 replacing the current Data Protection Act. The Solent SCITT is committed to protecting the privacy and security of your personal information. These protocols outline good practice guidelines for all stakeholders

Please refer to our privacy notice, which describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all employees, trainees, workers and contractors, but does not form part of any contract of employment or other contract to provide services.

The Solent SCITT is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

Policies

We have clear policies and guidelines covering the following:

- Privacy Notice
- Data Breach Response
- Public Access Requests

These policies are located at xx and all stakeholders are expected to read, understand and adhere to the recommendations made. For further information, or if you have any questions about these policies, please contact Philip Seery, SCITT Office Manager.

Protocols

The following recommended guidance should be adhered to by all stakeholders:

- Passwords should be strong, secure and not shared with others, including electronically
- Laptop, tablet and desktop screens should be locked by the respective user when not in use
- Avoid storing sensitive data on portable devices, including: memory sticks, hard drives, phones and tablets
- Email accounts should be confidential and not accessed by multiple users
- Where possible work/training email addresses should be used for SCITT correspondence

- SCITT issued security passes are the responsibility of the holder and should not be used by others
- Any confidential information is stored securely in the SCITT office and must not be removed
- Confidential information, for example: student data should be appropriately stored and not available for others to view
- Student data is highly confidential, should be anonymised where possible and should not be shared outside of the training context
- Obsolete confidential information must be shredded
- Consent for holding personal data including images will be obtained. An individual has the right to withdraw consent at any time
- We will respond to reference requests using held data
- Consent will be obtained when sharing personal data for marketing purposes
- Sensitive information shared, stored or sent electronically will be encrypted

Working Remotely

Due to the nature of the profession, we recognise that working from home is likely. It is imperative that school and SCITT protocols are adhered to at all times. Student data is highly confidential and should be treated as such. Individuals should take particular care when working in shared spaces and on shared devices. Individual laptops will be loaned for the duration of training and it is the trainee's responsibility to ensure equipment is used safely and appropriately.

Google Drive

The Google Drive is used as a central hub for the file sharing and storage of:

- SCITT email addresses
- Training resources
- Course information
- Tracking information

Access is limited to relevant stakeholders with permissions granted on an individual basis. Sensitive information is encrypted and permissions are reviewed on an annual basis.

External or third-party users

On occasion, it may be necessary to share information with external or third-party users for inspection or moderation purposes. Where possible, data will be anonymised and access to personal information will be appropriately restricted.