# Data Protection Policy - GDPR

## Rationale

ICON is committed to a policy of protecting the rights and privacy of individuals, including students, staff, host families and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how businesses manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

To comply with various legal obligations, including the obligations imposed on it by the GDPR, ICON must ensure that all information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

## General Data Protection Regulation (GDPR)

This piece of legislation came into force on the 25th May 2018. The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to and individual and may be in hard or soft copy (paper/manual files; electronic records; photographs) and may include facts or opinions about a person.

## Compliance

This policy applies to:

- The head office of ICON
- All branches of ICON
- All staff of ICON
- All contractor, suppliers and other people working on behalf of ICON

It applies to all data that ICON holds relating to identifiable individuals.

## Responsibilities under the GDPR

ICON will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of personal data.

Senior management is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the business.

Compliance with the legislation is the personal responsibility of all members of ICON who process personal information.

Individuals who provide personal data to ICON are responsible for ensuring that the information is accurate and up-to-date.

## Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles:

1. Process personal data fairly and lawfully
2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose
3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed
4. Keep personal data accurate, and where necessary, up to date
5. Only keep personal data for as long as is necessary
6. Process personal data in accordance with the rights of the data subject under the legislation
7. Put appropriate technical and organisational measures in place against unauthorised or lawful processing of personal data, and against accidental loss or destruction of data
8. Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

## Consent

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when ICON is processing any sensitive data, as defined by legislation.

ICON understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via application form) whilst being of sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

ICON will ensure that if the individual does not give their consent for the processing and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

## Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by ICON. Any individual wishing to exercise this right should apply in writing to the Managing Director.

Under the terms of the legislation, any such requests must be complied with within 40 days.

## Disclosure of Data

In certain circumstances the legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ICON will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking advice where necessary.

## Policy Review

ICON is committed to ensuring this policy remains fit for purpose, it will be reviewed annually and updated accordingly.

Next review date: 1.06.2019