The Institute of
Clinical Science & Technology

Data Protection Policy

1. Definitions

Data Controller:
The Institute as the Data Controller determines the purposes and the manner in which personal data is processed.

Data subject:
An employee, a student or a stakeholder whose personal data is processed by the Institute.

Notification:
This entails the Institute informing the Information Commissioner's Office of certain details about its processing of personal data. The main purpose of notification and the public register is to promote openness in the use of personal data.

Personal data:
Data that relates to the Institute's employees, students, and its other stakeholders.

Sensitive information:
This forms a subset of personal data and includes racial or ethnic origin, religious beliefs, and health and criminal convictions.

Subject Access Request:
employees, students and stakeholders can request to have copies of their personal data held by the Institute.

2. Introduction

The UK Data Protection Act 1998 (the Act) came into force in October 2001 as a result of the European Directive (EC) 95/46.

The Act applies to all personal data on computer or manual filing systems and places obligations on the Institute.

The Institute is therefore obliged to protect the personal data of its employees, students and stakeholders in accordance with the Act and its Notification to the Information Commissioner's Office.

This policy is formulated in line with the British Standard BS 10012:2009, Data protection: specification for a personal information management system.

3. The Data Protection Principles

The Data Protection Principles define how personal data can be legally processed.

In accordance with the Principles personal data has to be:

a) Processed fairly and lawfully

b) Processed for specified and lawful purposes

c) Adequate, relevant and not excessive;

d) Accurate and up to date;

e) Held no longer than is necessary;

f) Processed in accordance with the rights of the data subject;

g) Kept securely and

f) Not transferred outside the countries of the European Economic Area without adequate protection

4. Data security

The Institute and its employees are to ensure that all personal data is securely kept to avoid any unauthorised disclosure.

There should be no accidental disclosure, either orally or in writing, of personal data to any unauthorised third party.

Appropriate technical and organisational measures must be in place to ensure there is no unauthorised processing of personal data.

5. Scope of the policy

That the Institute ensures that its employees and students comply with the provisions of the Data Protection Act 1998.

That the Institute collects and processes personal data only to fulfil operational needs and to comply with its legal obligations.

That students and employees be reminded once a year to update any changes to their personal data.

That data audit is carried out once a year to ensure that processing of personal data falls within the purposes notified to the Information Commissioner's Office.

That all Information Representatives be of at least managerial level, to ensure that employees are aware of the requirements of the Act.

That employees carry out "weeding" exercises of their records once every two years to ensure old data has been removed from the system.

That the Principal be notified of changes made to existing information systems throughout the Institute.

That any personal data to be retained for long-term preservation is to be transferred to the Institute' Archives.

That any infringement of the Act will be treated seriously by the Institute and disciplinary procedures may follow.

6. Responsibilities

The Institute recognises its corporate responsibilities within this Policy as follows:

The overall compliance for this Policy lies with the Principal to whom the Institute's Data Protection Officer reports;

Directors of support departments are to ensure good personal data management in their respective areas in line with the Institute's Records Management Policy and to liaise with the Data Protection Officer on all matters relating to the Data Protection Act.

7. Subject Access Requests

All student, employees and stakeholders can make Subject Access Requests to the Institute Data Protection Officer for copies of their personal data in line with the Act. (See Appendix B for the detailed procedure).

8. Complaints

Complaints should be addressed to the Institute Data Protection Officer to deal with them in line with the Institute's Data Protection/Freedom of Information Complaints Procedure.

If complainants are dissatisfied with the outcome, they may seek an independent review from the Information Commissioner.

9. Training and Guidance Notes

All employees who handle personal data should receive training in the Act as part of the Staff Development Training Programme.

Guidance Notes necessary to help comply with this Policy will be made available to all staff by the Data Protection Officer.

An e-learning module on the Act has been made available by the Data Protection Officer, to be completed by all Institute staff.

10. Review of the Policy and the GDPA

On 25th May 2018 the UK Data Protection Act 1998 (the Act), will be replaced by a new, European-wide law, the General Data Protection Regulation (GDPR). Many of the GDPR's main concepts and principles remain, but the GDPR provides data subjects with enhanced rights and imposes increased responsibilities on ICST in their capacity as data controllers and data processors.

ICST is the 'data controller' for all personal data it holds and processes, except where this is carried out in its capacity as a 'data processor' on behalf of another data controller. In those circumstances the entity which provides the data is the 'data controller'. Under the new GDPA regulations, responsibility for ensuring proper data handling is spread between both data processor and data controller to provide greater safety for the data subject.

The GDPR strengthened requirements include increased transparency about how personal information is used and increased accountability from organisations from data controllers and processors, through robust procedures and good record keeping.

What are we doing to be compliant?

We have a dedicated team, led from the top, that has reviewed our current data protection practices against the new requirements coming into force in May. We have, for some time, been designing new projects with GDPR requirements in mind and are already implementing changes to existing projects. We will continue to update our practices and procedures as the deadline approaches. We are

a) Refreshing our privacy notices, documentation and website to ensure transparency about data processing.
b) Implementing explicit consents with regard to collecting sensitive data.
c) Developing processes to support the new rights for an individual who is the subject of personal data.
d) Developing processes to demonstrate that we are complying with data management requirements.
e) Developing processes to ensure we are notifying any data breaches to individuals affected and regulars within 72 hours.
f) Ensuring our IT and technology systems provide sufficient protection of personal data.
g) Educating and informing our colleagues on the changes we're making, including training.

Some of our procedures have already been updated, for example, see Use of Student Data and the GDPR

11. Further information

Any questions about Data Protection and ICST's response to GDPR can be directed to the Data Protection Officer, katie.dick@clinicalscience.org.uk