

## Data protection policy

### Introduction

1. The Royal College of Pathologists exists to promote excellence in the practice of pathology and to be responsible for maintaining standards through training, assessments, examinations and professional development, to the benefit of the public. It was incorporated in 1962, received its Royal Charter in 1970 and is a registered charity (No. 261035). The College is governed by an elected Council. It:
  - provides the infrastructure to support training in the pathology specialties
  - operates a quality-assured Continuing Professional Development (CPD) scheme, including an online CPD portfolio facility
  - provides advice on establishing, approving and maintaining training programmes
  - approves educational job descriptions and maintains a network of specialty advisors
  - has committees that steer the direction and offer advice to members of all the pathology specialties
  - conducts examinations for scientists and doctors wishing to specialise
  - provides ready access to the public perspective on pathology through the Lay Advisory Committee
  - organises conferences, scientific meetings and academic activities
  - collects workforce data and lobbies the UK governments on workforce issues
  - proactively approaches the UK governments and independent healthcare providers on pathology issues
  - distils guidance from government and other organisations, and publicises this to members
  - advises NHS and similar organisations, the independent sector and the public
  - provides a conduit for academic and research funding for studentships and fellowships
2. This data protection policy was approved by the College Council on 6 June 2013.
3. The College reserves the right to modify this policy at any stage. It will be reviewed when necessary.

### Guiding values

4. In order to conduct its normal business, the College collects and uses certain types of personal information about living individuals. These include current, past and prospective Fellows, and members, staff, suppliers, clients, customers, and others with whom it has business or with whom it communicates. The College will only collate and hold personal information that is essential for College business (see 'Data protection principles' below).



5. The College considers the lawful and correct treatment of such personal information as essential to the efficient and successful conduct of its business. It also recognises that correct and lawful treatment of personal information is crucial to fostering and maintaining the confidence of its main stakeholders and the wider public in the College and its operations.
6. The College is committed to ensuring that it treats personal information lawfully and correctly, and recognises that there are safeguards to ensure this in the Data Protection Act 1998.

### **Data protection principles**

7. The College fully endorses and adheres to the Principles of Data Protection, as enumerated in the Act. These are that:
  - personal information shall be processed fairly and lawfully and shall not be processed unless certain conditions (*the following*) are met
  - personal information shall only be obtained for specified and lawful purposes and not be further processed in a manner incompatible with those purposes
  - personal information shall be adequate, relevant and not excessive for the purpose(s) for which it is processed
  - personal information shall be accurate and, where necessary, kept up to date
  - personal information shall be kept for no longer than necessary for those purposes
  - personal information shall be processed in accordance with the rights of data subjects
  - appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss of, or damage to, personal data
  - personal information shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

### **Organisational and management controls**

8. The College will put in place appropriate management and organisational controls in order to:
  - observe fully conditions regarding the fair collection and use of personal information
  - meet its legal obligations to specify the purposes for which such information is used
  - collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs, or to comply with any legal requirements
  - ensure the quality of personal information used
  - apply strict checks to determine the length of time personal information is held
  - ensure that the rights of people about whom information is held can be fully exercised, including:
    - the right to be informed that processing is being undertaken
    - the right of access to one's personal information
    - the right to prevent processing in certain circumstances
    - the right to be told how that information is being used
    - the right to be told the source of that information

- the right to be told about any other person or body to whom that information is disclosed
- the right to correct, rectify, block or erase information which is regarded as wrong information
- take appropriate technical and other security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards
- carry out regular assessments of compliance with the Data Protection Act 1998.

### **Staff supervision, awareness and training**

9. The College will also:

- appoint someone with specific responsibility for data protection (currently the Head of Operations)
- ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- describe clearly methods of handling personal information
- arrange for appropriate training for everyone managing and handling personal information
- supervise appropriately everyone managing and handling personal information
- ensure that staff deal with queries about personal information promptly and courteously
- conduct a regular review and audit of the way personal information is managed
- assess and evaluate regularly methods for handling personal information.