Data Protection Policy

Introduction

The Society needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective employees, Trustees, Committee members, members, suppliers and others with whom it communicates.

The purpose of the Data Protection Act 2018 (referred to as the 'Act' throughout the remainder of this policy) is to protect individuals' rights to privacy and confidentiality regarding their personal and financial affairs and place obligations on those processing personal data to manage that data lawfully. The Act works in two ways:

- it gives individuals rights in relation to their personal data; and
- requires those who process personal data to follow certain practices

This Data Protection Policy sets out both the Society's responsibilities and staff/contractors (incl. PCRS Leads) responsibilities under the Act. Failure to comply with the Act could result in prosecution of not only the Society but also of the staff/contractors (incl. PCRS Leads) involved and breach of the Policy, whether deliberate or through negligence, could lead to disciplinary action.

Responsibility for Data Protection

The Chief Executive acts as the individual with overall responsibility for Data Protection for the Society and has overall management responsibility for Data Protection. She also acts as the contact person for queries.

However, all staff/contractors (incl. PCRS Leads) are responsible for ensuring that they process personal data in accordance with the Act and all staff/contractors (incl. PCRS Leads) must familiarise themselves with this Data Protection Policy and comply with it. In addition all staff/contractors, (incl. PCRS Leads) must familiarise themselves with and abide by the PCRS:

- 'Bring your Own Device' (BYOD) policy
- Privacy policy for members, those registering for and attending events, affiliated group leaders and others interacting with the Society
- Privacy notice for staff, trustees & committee Members

If any staff/contractors (incl. PCRS Leads) member has any questions relating to Data Protection, they should contact the Chief Executive for guidance.

Personal Data

Personal data is defined as information relating to an identifiable living individual and can be in any format, electronic (including websites and e-mails), paper-based, photographic etc. from which the individual's information can be readily extracted.

The definition of personal data is very wide, and staff/contractors (incl. PCRS Leads) should assume that any information held about a living person, including expressions of opinion, is personal data.

Processing

Personal data is covered by the Act if it is processed. The definition of processing is also very wide. It covers virtually every use of personal data, including obtaining data; holding it in any way; looking at it on a screen, using it; disclosing it to a third party; and even disposing of it. Staff/contractors (incl. PCRS Leads) should assume that any activity associated with personal data constitutes processing and is covered by the Act.

Processing should only be carried out when the processing is fair and legal and the following conditions have been met:

- the purposes are valid;
- the purposes can only be achieved by processing the personal data;

- the processing is proportional to the purposes;
- the person has not been misled or deceived when the data was obtained;
- the data subject has been notified (where required)

Staff/contractors (incl. PCRS Leads) should also only process data when it is necessary for the performance of a contract or agreement, necessary for the legitimate interests of the Society, or in some cases a third party, and can be carried out without prejudicing the interests of the person concerned, or where the Society has the individual's specific (or in the case of sensitive data, explicit) consent to do so. Staff/contractors (incl. PCRS Leads) should therefore be clear about the justifications for processing data and seek advice from the Chief Executive if required.

Staff/contractors (incl. PCRS Leads) should ensure that individuals are aware that the Society is processing their data, the purpose for which they are processing that data and where relevant that the individuals have given their consent to the processing of that data. Note that electronic communication with an individual, other than where it is in direct response to an electronic request for information from them or is in performance of a contract or agreement with them (where the terms of that contract or agreement have made clear that electronic communication will be involved), will almost always require their specific consent. See Sensitive Data below where express consent is necessary.

The Data Protection Principles

The Act requires the data to be processed in accordance with the data protection principles:

- be processed fairly and lawfully
- be obtained only for lawful purposes and not be further processed in any manner incompatible with those purposes
- be adequate, relevant and not excessive
- be accurate and where necessary kept up to date
- not be kept longer than is necessary for its purpose
- be processed in accordance with the data subject's rights
- be secure
- not be transferred to countries outside of the European Economic Area (EEA) without adequate protection

Staff/contractors (incl. PCRS Leads) must make themselves familiar with the above principles and ensure that they process data in accordance with them.

Purposes for Processing Data

Staff/contractors (incl. PCRS Leads) should ensure that they are familiar with the purposes for which the Society processes personal data, and that no data is processed for any other purpose.

The Society is registered as a data controller under register entry Z8305954. The Society has registered the following purposes for which it processes data:

"We process personal information to enable us to administer our membership records and activities including fundraising; maintain our own accounts and records; support and manage our staff and volunteers."

The Society will keep the purposes for which it processes personal data under review and if those purposes expand beyond those listed above it will notify the Information Commissioner. Staff/contractors (incl. PCRS Leads) should notify the Chief Executive immediately if they anticipate processing personal data for any other purposes or if they have any queries as to what falls within the registered purposes.

Sensitive Data

The Act makes special provision in relation to sensitive data. This is data about racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; and criminal proceedings or convictions. In addition to the conditions relating to all personal data, sensitive data can only be processed if it is necessary and the Society:

- has the explicit consent of the person concerned, or
- is required by law to process the data for employment purposes, or
- needs to protect the vital interests of the person, or another (and it is not feasible to obtain consent); or
- is aware that the information has already been deliberately made public by the person concerned; or
- is using the information for equal opportunities monitoring; or

- is using the information for the administration of justice or legal proceedings (unlikely to arise).

Staff/contractors (incl. PCRS Leads) must therefore take extra care in relation to the processing of sensitive data and know that one of these conditions is met. If explicit consent is required, this must be in writing, and must be kept for as long as the sensitive data is held. For explicit consent the person should receive specific information about the processing of the data, and its purpose. Consent should not be inferred from a non-response, or requiring a data subject to "opt out".

Staff/contractors (incl. PCRS Leads) should also take extra care to ensure that sensitive information is kept secure and only seen by those who have a legitimate reason to see it. See Data Security below.

Disclosures of Data

Staff/contractors (incl. PCRS Leads) should only disclose personal data to third parties if the data subject has consented; if the Society is under an obligation by law or contract; or if it is necessary for the performance of a contract or agreement between the Society and the data subject. The unauthorised disclosure of personal data is both a contravention of the Act and a breach of confidentiality. Therefore, care must always be taken to ensure that any disclosure is fair and lawful and if in doubt you should refer to the Chief Executive for guidance.

Also, the identity of any person seeking access to personal data must be confirmed before a disclosure is made. If staff/contractors (incl. PCRS Leads) have any concerns about the identity of a person requesting personal data, they can seek advice from the Chief Executive before a disclosure is made.

Quality of Data

Staff/contractors (incl. PCRS Leads) should undertake the following measures in relation to all personal data:

- Identify the minimum amount of information that is necessary
- Ensure that information held is relevant, and necessary, for each person that it is held for. Staff/contractors (incl. PCRS Leads) should not hold information for a group of individuals when it is only necessary for some of that group
- Be aware in recording statements of opinion that these are personal data, and should only be held if necessary
- Not hold data on the basis that it might be useful in the future, without a clear view as to how it will be used;
- Take all reasonable steps to ensure the accuracy of data
- Keep personal data up to date (except where it is held for historical reasons) and review it on a regular basis
- Keep a record of the date on which personal data is recorded, or updated
- Take care to ensure that personal data held on computer (for example on emails) is held for no longer than is necessary.

Personal data that is no longer active should only be held if it is necessary for the management of the Society to keep a record of past actions; for monitoring purposes; or in case of legal proceedings.

Data Subject Rights

The Society will respect the protective rights of the data subject (that is the person about whom the data is held), which are established under the Data Protection Act. Individuals have the following rights under the Act:

- To know that their personal data is being processed, why it is being processed and to whom it is being disclosed
- To make access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision taking processes that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To take action for compensation if they suffer damage by any contravention of the Act
- To take action to rectify, block, erase or destroy inaccurate data
- To request the Information Commissioner to assess whether any provision of the Act has been contravened
- To require us to correct the personal data we hold about them if it is incorrect
- To require us to erase their personal data

- To require us to restrict our data processing activities (and, where our processing is based on their consent, they may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal)
- To receive from us the personal data we hold about them which they have provided to us, in a reasonable format specified by them, including for the purpose of transmitting that personal data to another data controller
- To object, on grounds relating to their particular situation, to any of our particular processing activities where they feel this has a disproportionate impact on their rights.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply. Where a data subject seeks to exercise their rights under the Act, staff/ contractors (incl. PCRS Leads) should always seek advice from the Chief Executive before taking action.

Subject Access Requests

Any living person about whom the Society holds data has the right to make a Subject Access Request. In addition, they are entitled to have access to certain personal data that the Society is processing.

All Subject Access Requests must, in the first instance, be referred to the Chief Executive. Staff/contractors (incl. PCRS Leads) should be aware that a Subject Access Request may not initially be in writing. Any request by any person for any personal data should be regarded as a Subject Access Request. If the initial request is not in writing, the person must be immediately asked to put the request in writing, or the request must be forwarded directly to the Chief Executive who will do so. However, the fact that a request is not made in writing must never be used as a means of delaying the response. The Society is obliged to fully respond to any Subject Access Request within one month.

Subject Access Requests can be made by a wide range of people. It should never be assumed that the Society does not hold personal data about a person; all requests must be passed to the Chief Executive.

If the Society does not respond correctly to a data subject access request or is unlawfully processing data, the Information Commissioner may issue a notice or obtain a Court Order. Any notices or Court Orders, relating to a person's rights under the Act should be forwarded to the Chief Executive immediately.

Requests will be responded to free of charge unless repetitive or numerous in which case a reasonable administrative fee may be charged; this should be discussed with the Chief Executive.

Data Security

All staff/contractors (incl. PCRS Leads) are responsible for ensuring that any personal data they hold is kept securely. This will include:

- Using password protection on computers. Passwords should be changed regularly. Staff/contractors (incl. PCRS Leads) should not share passwords, and each new member of staff/contractor (incl. PCRS Leads) (including temporary staff/contractors should have a new password
- Ensuring tapes or discs are cleaned before reuse, rather than just writing over old data
- Keeping confidential personal data (in paper format) in secure locked cupboards
- Ensuring live data held on computer is not used for testing or sampling purposes. If actual data must be used (as opposed to dummy data) this must be a test copy only
- Ensuring that data is used for the Society's purposes only. The processing of personal data for any unauthorised purpose may lead to disciplinary action.
-

Personal Data Breach

A personal data breach means a breach of security from either accidental or deliberate causes leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes any security incident that affects the confidentiality, integrity or availability of personal data. A personal data breach occurs whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Any member of staff/contractors (incl. PCRS Leads) who become aware of a security incident must report it immediately to the Chief Executive who is responsible for establishing whether a personal data breach has occurred and if so, promptly take steps to contain and address it, including:

- Establishing the likelihood and severity of the resulting risk to people's rights and freedoms;
- Notifying, the Information Commissioner's Office (ICO), within 72 hours of becoming aware of the breach if there is likely that there will be a risk to individual's rights and freedoms;
- Informing without undue delay those individuals whose rights and freedoms, are at risk of being adversely affected;
- Ensuring the incident is recorded and documented.

Reviewed by PCRS Executive: **May 2021**
Approved by PCRS Trustees: **March 2018, July 2021**
Date of next review: **April 2024**

The Primary Care Respiratory Society UK registered office: Miria House, 1683b High Street, Knowle, Solihull B93 0LL.
Registered Charity: 1098117 Company No: 4298947 VAT Registration Number 866 1543 09
Telephone: +44 (0)1675 477600 Email: info@pcrs-uk.org Website: http://www.pcrs-uk.org

We are grateful to our corporate supporters for their financial support which supports the core activities of the Charity and allows us to make our services either freely available or at greatly reduced rates to members. PCRS statement on pharmaceutical funding