

Society guide to the Data Protection Act and individual rights of its members and the general public

Important policy extracts

The rights under the Data Protection Act (DPA) for members and staff of the Society and the general public are the same and no privilege is afforded to any grade of membership.

Whilst this document is provided primarily to inform all individuals of their rights under the DPA with regards to the Society's services, it is important to note at this early stage that the Society as a registered charity is the Data Controller. Only contracted and authorised staff or authorised third parties can act on behalf of the Society in the collection, processing, storage, security and deletion of the personal and sensitive data collected for the purposes in administering the Society's aims as set out in its Royal Charter and on-going strategies.

As members of the Society are not contracted employees of the Society they are not permitted to access, collect and use or store any data protected by the DPA which is collected and stored by the Society's authorised employees or on behalf of the Society by authorised third parties.

However, under some special projects and circumstances, members with appropriate skills will be contracted under a "Contract for Services" to work for the Society and where personal or sensitive data access is required a "Data Sharing Agreement" and/or a "Non-Disclosure Agreement" between the Society (Data Controller) and the member (Data Processor) will be required in advance before the member is authorised to access or collect the data.

For the benefit of doubt, these guidance and statements of policy do not restrict any members of the Society from collecting, processing or storing personal or sensitive data for the purposes of their employer or their own practise, but it is recommended that members ensure that full compliance with the DPA is in place by their employer or that they have the required compliance as a self-employed practitioner.

All employed staff of the Society are required to complete a basic DPA training course when joining the Society, followed by refresher courses every three to five years. Access to data cannot be given to any non-employed members, as this presents an uncontrollable data security assurance challenge. However, there are dedicated staff and secure systems available for all members to communicate within their group where informed consent has been granted.

Guidance explaining individual rights under Data Protection

Individual Rights

1. An individual's (the Data Subject) rights under the Act include the following:
 - a) right to be informed if a Data Controller is processing their personal and/or sensitive data;
 - b) right to subject access;
 - c) right to prevent processing likely to cause damage or distress;
 - d) right to prevent processing for purposes of direct marketing;
 - e) rights in relation to automated decision making;
 - f) right to sue for compensation, rectification, blocking or destruction of data if an individual suffers damage or distress by any breach of the DPA by the Data Controller;
 - g) right to take action to rectify, block, erase or destroy inaccurate or obsolete data;
 - h) right to privacy.

What is Personal data?

Personal data is any data that identifies a 'living' individual. For example; a name on its own is not personal data, but a name and address combined can identify an individual, thus it becomes personal data. Therefore any data about a living, identifiable individual, either on its own or in combination with other data held by a Data Controller is personal data. To process personal data protected by the DPA the Data Controller must ensure that at least one of the following conditions (schedule two of the DPA) is met:

- Consent is given by the Data Subject and that it is informed, freely given and specific.
- That the data is necessary to fulfil a contract.
- There is a legal obligation to process the data.
- It is necessary to protect vital interests.
- That the Data Controller is a legal power or public function.
- That legitimate interests can be demonstrated to process the data.

What is sensitive data?

Sensitive data includes information processed about an individual that falls within the following subject areas:

- race and ethnic origin
- politics
- physical and mental health
- current criminal proceedings
- criminal offences
- religious and philosophical beliefs
- sex life and sexual orientation
- trade union membership

At least one of the following additional conditions (schedule three of the DPA) must also be met for a Data Controller to process an individual's sensitive data:

- Explicit consent from the Data Subject – e.g. consent or response for the voluntary collection of member ethical data (i.e. ethnic origin, health disability etc.) to support improving member benefit services.
- Employment rights/obligations apply – e.g. health data to ensure appropriate adjustments can be provided at educational courses and event venues.
- Use by groups defined by sensitive characteristics – e.g. ethnic origin data or criminal offences for use within specific authorised psychologist groups (Race and Culture, Forensics etc.), to enable appropriately represented research and methods.
- The Data Subject has put data into the public domain – e.g. A Data Subject runs a blog which contains their sensitive data.

Right to be informed and give informed consent

All individuals have the right to be informed about the data that any organisation collects about them where it is considered necessary to do so in the interest of the organisations publish aims, services and processes.

The main process for collecting personal data from members and the general public for the Society is through informed opt-in consent wherever necessary to do so. On occasion, implied or reasonably expected consent is assumed provided that the appropriate DPA conditions are met. For example, where it is a basic requirement of a routine membership application (i.e. there are certain basic data elements such as name, address and qualifications that are fundamentally required to enrol an individual into membership of a learned society) and that there is no compromise of expected confidentiality or human rights. However, the intended use of the data will be explained on the application form.

As is currently required within the DPA from all Data Controllers, the Society has informed the Information Commissioner Office (ICO) through the standard 'notification' process confirming the data we collected and how it is processed and used. This notification is freely available to view on the [ICO website](#) – registration number Z5958155.

Subject Access

Any individual has the right to access their personal data processed by an organisation through a Subject Access Request (SAR). You cannot request the personal data of any other individual unless you can prove you are an agent acting on their behalf with consent. The Society will require reasonable levels of proof of identity to ensure you are who you say you are. A fee may apply up to the value prescribed by the ICO at the time of the SAR.

Data subjects have the right to:

- personal data
- the purposes for which the data are being processed
- to whom the data may be disclosed
- how the data is stored and secured (without compromising specific security methods)

Subject Access continued

Data must be intelligible and provided in a permanent form.

A response to a subject access request must be made within 40 days from the date of acceptance of proof of identity and fee receipt.

Disclosures relating to the physical or mental health condition of the data subject should not be made without consulting an appropriate health professional.

Information relating to a third party will only be disclosed if the third party has consented to disclosure or where it is reasonable to do so in all circumstances to comply with the DPA and deemed by the Society to be fair, uncontentious and without causing potential damage or distress. Requests can be made by an agent of the data subject. It is necessary in such cases to be satisfied that the subject's agent is acting on behalf of the data subject.

The Society's formal protocol for SARs can be obtained from the BPS offices. Our staff are trained to be aware that SARs may be identified through conversation, indication in correspondence/email, via Social Media or any other form of communication and that they advise that a formal request is submitted in writing to the [Data Protection Officer](#) and that a fee applies (where appropriate).

Response to an SAR

The Society will respond to SARs following proof of identity and receipt of a fee (where appropriate) as required by the DPA and dependant on the detail of your request, by:

- Clarifying the requirements of your request where necessary
- Searching all information management systems, including but not limited to databases, email systems, member network repositories, back-up records and storage networks
- Searching structured filing systems
- Provide the data held on you in a permanent form (printed and sent by secure post)
- Explain the data and the purpose of why it is processed where necessary
- Advise on any data withheld or redacted and the reasons for this
- Make reasonable adjustments for Data Subjects with special requirements due to disability
- Respond within the 40 day time limit required by the DPA/ICO.

Subject Access continued

If the information held on you also contains personal information of someone else, this may be redacted or withheld following due care and attention by the Data Controller to the following considerations:

- Is the third party identifiable? – e.g. an identifiable referee who has provided a confidential reference for a membership application
- Does a duty of confidentiality apply to the third party?
- Can consent be obtained from the third party? – e.g. is it possible and reasonable to contact the third party for consent without prejudicing a lawful or tax investigation or breaching the confidentiality of the data subject making the SAR
- Is it reasonable and feasible to remove the third party from the data to accurately respond to a SAR
- Is it reasonable and correct to disclose the third party data without consent in the SAR response - e.g. the third party may now be deceased?

Right to prevent processing likely to cause damage or distress

In most cases this is unlikely to occur in relation to the kind of data the Society holds. Possibilities for where such data may arise include;

- membership – we will take all reasonable measures to comply with your request and explain any consequence of such an action, such as, being unable to remain a member or removal from a Society register without your consent to maintain your basic personal data.
- qualification supervisors reports – if a request to prevent processing was received we would need to consider this in light of the principles of the Act, including whether the processing is necessary for the performance of our contract with a candidate and to provide a written notice within 21 days advising that we were complying with the request or, if not, why not.
- a claim for extenuating circumstances – again a request would need to be considered in light of the principles of the Act and the circumstances of the claim.

Prevention of processing for the purposes of direct marketing

Whilst the Society never provides data to third parties for marketing purposes, we do work with outsourced companies to provide specialised and specific services. All third party companies employed by the Society are subject to our data sharing and non-disclosure agreements and only authorised to process data that is relevant to their service. The companies use the Society data systems directly through secured and authorised access routes and no data is stored on their own systems.

We do process our own direct mailing services to approved third parties from time to time and these materials are only dispatched to members who have consented by opting in to these on-line and postal services.

Effectively all data protected by the DPA for members and public subscribers remain only on Society information systems.

Right to compensation

Where an individual suffers damage or distress as a result of any proven breach of the DPA they are entitled to sue for compensation. This would be decided by the courts, unless a mutual settlement can be reached.

This may be a factor in exams. For example, if a contravention resulted in a delay to a candidate's qualification, and this had a direct link to the salary paid by their employers, then compensation may be payable.

Example: A candidate notifies the Society of an address change and this is logged on the Society's database. In the unlikely event that a contracted registrar is not made aware of the change of address and they write to the candidate at their previous address, which is now inaccurate. The candidate does not receive the letter and, as a result, does not have vital information relating to a required submission and therefore, fails to submit appropriate material for the examination. The candidate's qualification is delayed by 12 months and their employer does not pay the higher rate salary until the qualification is awarded. The candidate would be able to demonstrate a loss and could therefore be entitled to compensation.

Right to take action to rectify, block, erase or destroy inaccurate data

A data subject may apply to the court for an order requiring the data controller to rectify, block, erase or destroy such data relating to the data subject which is inaccurate, together with any other personal data relating to the data subject which contains an expression of opinion which the court finds is based on the inaccurate data. Data are inaccurate if they are incorrect or misleading as to any matter of fact.

The court could rule that damage has been caused by inaccurate data and award compensation.

The data controller may be required to notify third parties, to whom the data has been disclosed of the rectification, blocking, erasure or destruction of the data.

If the court is satisfied that the data controller has taken reasonable steps to ensure the accuracy of the data then the court may, as an alternative, order that the data be supplemented by a court approved statement of the true facts.

Exemptions and modification

The DPA makes provision for certain exemptions for non-disclosure. Exemptions that relate to various processes and situations of the Society are as follows in brief below:

- Crime prevention – where a potential crime or tax collection investigation may be deemed to be obstructed if the data is not disclosed on request
- Research – see explanation below
- Regulatory activity – where disclosure to a regulatory authority may occur to protect the public
- Health and education – in the interests of providing support for educational services that require qualified/authorised member support
- Statutory purposes – as required by the HCPC in the case of the Society to ensure public safety
- Disclosure required by law
- Disclosure for legal proceedings

All requests for data relating to the above exemptions are carefully assessed in respect of the provisions of the DPA and verified/authorised before a response is considered. These are not taken on face value only.

Other exemptions from subject access requests

The DPA makes provision for certain data exemptions from Subject Access Requests that relate to the Society processes, as follows:

- Confidential references provided by and to the Society for membership and educational purposes.
- The corporate finances and management forecasts of the Society
- Examination scripts and marks - explanations below.

In each case the data controller is required to consider the nature of the request, the information and how far the provisions of the exemption order apply.

Research

The DPA provides for various exemptions in respect of processing of personal data for research purposes provided that the processing is exclusively for those purposes and also, that the following conditions are met:

- The data are not processed to support measures or decisions relating to particular individuals; and
- The data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.
- Where the exemptions applies:
- the further processing of personal data will not be considered incompatible with the purposes for which they were obtained; and
- personal data may be kept indefinitely despite the Fifth Data Protection Principle; and
- subject access does not have to be given provided that the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

It is important to note that even where the exemption properly applies we are still required to comply with the rest of the Act, including the First and Second Principles (processing data fairly and for notified purposes respectively). The Society will therefore ensure that, at the times the data are collected and processed in compliance with the DPA and the data subject is made fully aware of what the data controller intends to do with the data. If the data controller subsequently decides to process the data in order to carry out further research of a kind that would not have been envisaged by the data subject at the time the data were collected, then the data controller will need to comply with the fair processing requirements of the Act in respect of this further processing.

As a matter of good practice, when processing for research, historical or statistical purposes, the Society will always consider whether it is necessary to process personal data in order to achieve their purpose. Wherever possible, the Society will only process data that has been stripped of all identifying features.

Examination scripts

Where personal data consists of information recorded by candidates during an examination they are exempt from subject access. However, any comments recorded by the examiner in the margins of the script are not exempt and as such should be provided even though they may not appear to the Society (the data controller) to be of much value without the script itself.

Examination marks

This is not an exemption as such but rather is an adaptation of the requirements in section 7 of the DPA to comply with a subject access request within the specified 40 day response time. In the case of a subject access request made in relation to examination marks or results, the timescale will be delayed if the date of the request precedes the date of publishing the examination results. This delay will be extended to either:

Five months from the day on which the data controller received the request; or 40 days from the announcement of the examination results; whichever is earliest.