**Anatomical Society – Data Protection Policy**

**Key details**

* Policy prepared by/updated by: Anatomical Society Council
* Approved by council on: 12.07.22
* Policy became operational on: 12.07.22
* Last reviewed: 12.07.22
* Next review date: July, 2023

**Introduction**

The Anatomical Society needs to gather and use personal data about individuals from time to time. This can include, but is not limited to, personal data about people who apply to join the Society, its current or previous members, employees, trustees, consultants, partners and anyone that wishes to participate in any activity organised by the Society.

This data protection policy describes how and why personal data is processed by the Anatomical Society. When we talk about **processing** in this policy we mean any activity that involves the use of personal data. Processing includes obtaining, recording or holding personal data, or carrying out any operations on the data such as organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes sharing or transferring personal data with third parties collected, handled and stored.

The aim of this policy is to ensure that the Anatomical Society:

* Complies with data protect law and follows good practice
* Protects the rights of everyone whose personal data is processed
* Is open about how it stores and processes individuals’ personal data
* Protects itself from the risks of a data breach

This policy applies to all employees, workers, volunteers, consultants, trustees and anyone else working for or on behalf of the Anatomical Society. It does not form part of any contract of employment or other contract for services and we may amend it at any time. You must comply with this policy when you handle personal data on behalf of the Anatomical Society.

**Responsibilities**

Everyone who works with the Anatomical Society has some responsibility for ensuring that data is collected, stored and handled appropriately. The Anatomical Society will facilitate councillors and staff who handle personal data to receive appropriate data protection training on induction, with regular refresher training thereafter.

The Anatomical Society council is ultimately responsible for ensuring that the Anatomical Society meets its data protection obligations.

If you have any questions about this policy, or if you have any concerns about how the Society is processing personal data, contact: maryanne.piggott@kcl.ac.uk or telephone 0207 848 8234.

**Data Protection Law and key terms**

The Anatomical Society must comply with UK data protection law, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR).

When we talk about **personal data** we mean any information which relates to a living person who can be identified from that data either on its own, or when taken together with other information which is likely to come into our possession. It includes identifiers such as a person’s name or ID number and expressions of opinion about a person’s actions or behaviour. The Society processes personal data about members and non-members such as employees, award holders, training programme participants, delegates to meetings, and individual contacts at supplier or partner organisations such as the RSB, Wiley-Blackwell, and Webree.

We use the term **special category data** to mean personal data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

**Criminal offence data** means personal data relating to criminal convictions and offences (for example, information about criminal activity, allegations, investigations and proceedings) and can include information about unproven allegations and information relating to the absence of convictions. It also covers related security measures, such as personal data about penalties and conditions or restrictions placed on an individual as part of the criminal justice process.

Personal data includes data where the information that identifies the individual has been replaced by a key or code that is kept separately (pseudonymised personal data).

Personal data does not include anonymous data, i.e. data that has had the identity of an individual permanently removed.

**What does the law cover?**

The Anatomical Society will comply with the data protection principles set out in the UK GDPR, which require personal data to be:

1. processed **lawfully, fairly and in a transparent manner**;
2. collected only for **specified, explicit and legitimate purposes**;
3. **adequate, relevant and limited** to what is necessary for the purpose it is processed;
4. **accurate** and where necessary kept up to date;
5. not be kept in a form which permits identification of the individual for longer than is necessary for the purpose it is processed (**storage limitation**);
6. processed in a manner that ensures its **security** using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Whenever the Anatomical Society processes personal data, we must take responsibility for what we do with it and we must keep sufficient records to be able to demonstrate our compliance with these principles. This is known as the accountability principle.

Each principle is explained below, together with a brief summary of how the Society complies with the principle in practice.

**Principle 1: fair, lawful and transparent**

We must only process personal data for specified lawful purposes. Depending on what we are doing with people’s personal data, the Society will rely on one of the following lawful purposes:

* the individual has given their consent to the processing;
* the processing is necessary for the performance of a contract we have with individual;
* the processing is necessary in order to meet our legal obligations;
* we need to process the data in an emergency to protect someone’s vital interests; or
* to pursue our legitimate interests (as long as those interests are not overridden by the interests or fundamental rights and freedoms of the individual).

When we process special category data or criminal offence data we need to have an additional lawful purpose. We will sometimes ask an individual to give their explicit consent to us processing these types of data, or we may rely on another purpose, for example where the processing is necessary:

* to carry out obligations or exercise rights in the field of employment, social security, or social protection law;
* for reasons of substantial public interest such as preventing fraud or safeguarding; or
* to protect someone’s vital interests if the individual is physically or legally incapable of giving their consent.

Our privacy notices contain more detailed information about the lawful purposes that the Society uses to process personal data.

Whenever we collect personal data directly from an individual, we must give them a copy of our relevant privacy notice. If we collect personal data from a third party or from a publicly available source, we must provide the individual with a copy of our privacy notice as soon as possible and not later than one month after we collect their personal data.

**Principle 2: specified, explicit and legitimate purposes**

You must only process people’s personal data for specified, explicit and legitimate purposes and you must not use their personal data in any way that is incompatible with those purposes.

Our privacy notices explain how and why the Society will use people’s personal data. If you want to use personal data for new or different purposes, we may first need to inform the individual and obtain their consent.

**Principle 3: adequate, relevant and not excessive**

You must only process personal data if you need it for the work you do for, or on behalf of, the Society and you are authorised to do so. You must not process personal data for any reason unrelated to your duties.

You must not collect more personal data than you need and you must ensure that any personal data collected is adequate and relevant for the intended purposes. You should not make unnecessary copies of personal data.

You should regularly review and update personal data which you have to process for Society business. When personal data is no longer needed for the specified purposes, it must be deleted or anonymised (see below).

**Principle 4: accurate and, where necessary, kept up- to-date**

You should check the accuracy of personal data when you first collect it.

We check the accuracy of the personal data we hold about members at least once a year on renewal of membership. If you become aware of inaccurate personal data you should take steps to steps to amend or delete the out of date personal data without delay.

**Principle 5: storage limitation**

We must not keep personal data in an identifiable form for any longer than is necessary for the purposes we collected it.

* Financial records are kept for 6 years.
* Certificates of Employers Liability Insurance are kept for 40 years.
* Governance records, a fixed asset register and annual trustees reports and accounts will be kept permanently.
* We keep all other personal data for 20 years.
* We keep a record of Anatomical Society staff, trustees and member names and affiliations in the historical records of the Society unless an individual requests that these be erased.

**Principle 6: security**

We have in place safeguards to ensure that we process personal data securely and to protect against unauthorised or unlawful processing, accidental loss, destruction or damage. We have back-up procedures in place to ensure that we can recover personal data in the event of computer failure or cyber-attack.

You must take reasonable and appropriate security measures when you process personal data on behalf of the Society. You should exercise particular care to protect special category data and criminal offence data.

You must follow procedures to make sure that personal data in filing cabinets and held on computer systems cannot be accessed by unauthorised personnel.

Hard-copy documents:

* When personal data is stored on paper it should be kept in a secure place where no unauthorised people can see it. This also applies to print outs of electronic data.
* When not required, paper documents or files should be kept in a locked drawer or filing cabinet.
* Hard copy print-outs should be shredded and disposed of securely when no longer required.

Data is stored electronically:

* Use strong passwords and change passwords regularly.
* Do not shared passwords.
* Data are stored on removable media (e.g. CD, disk drives etc.) should be encrypted and locked away securely when not in use.
* Personal data should be stored on designated drivers and servers and should only be uploaded to an approved cloud computing services.
* Servers containing personal data should be sited in a secure location.
* Data should be backed up frequently and backups should be tested regularly.
* Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
* All servers and computers containing data should be protected by an approved security software and a firewall.
* When working with personal data, all councillors and staff should ensure the screens of the computers are always locked when left unattended.
* Personally data should not be shared informally. Where access to confidential data is required, employees should request it from the designated person who has responsibility for permitting access to that data.
* Personal data must be encrypted being transferred electronically.

People attending Anatomical society meetings will be instructed that there is to be no unauthorised visual reproduction and dissemination of material from meetings (e.g. lectures, presentations, posters, exhibits) into the public domain (including social media) in order to comply with data protection and confidentiality principles.

**Photos and images**

When a delegate registers for an Anatomical Society meeting they are informed that photos may be taken in which they could be identified, and that the photos may be used for Society marketing and publicity purposes on legitimate interests grounds. Note that people have the right to object to legitimate interest processing (see below).

By submitting an image/image for an Anatomical Society Prize, an individual confirms that they have obtained permission from people who can be identified in any photos and that they agreed to the photos being used on the Anatomical society website/newsletter and other media. Individuals submitting an image for an Anatomical Society Prize will also be required to confirm that they own the copyright in the image or have gained explicit permission from the copyright holder for the image to be submitted for a specific award and to be used on the Anatomical society website/newsletter and other media. Applicants will be asked to agree to the following statement: *“I consent to the Anatomical society processing and storing my personal data that is associated with this application.”.*

**International transfers of personal data**

Data protection law places restrictions on transfers of personal data to countries outside the UK. This is to ensure that the level of protection afforded to people’s personal data in the UK GDPR is not undermined.

There are safeguards which to allow us to lawfully transfer some personal data to countries outside the UK. These include:

* transfers to countries that the UK has designated as providing an adequate level of protection for people’s rights and freedoms;
* transfers to third parties that entered into approved contracts with us covering the transfer;
* exceptional circumstances where the individual has given explicit consent to the transfer after being informed of any potential risks;
* where the transfer is necessary for one of the other limited reasons set out in data protection law, including the performance of a contract between us and the individual.

You must not transmit or send personal data to a different country, or allow people outside the UK to view or access our personal data, unless you are confident that one of these safeguards is in place.

**Data protection impact assessments**

The Society must undertake a data protection impact assessment (**DPIA**) if we plan to process personal data in a way that is likely to result in a high risk to individuals. It is also good practice to conduct a DPIA for major projects which will require us to process personal data.

We will usually conduct a DPIA when we implement major system or business change programs which involve processing personal data, such as:

* use of new technologies (programs, systems or processes), or changing technologies;
* automated processing (including profiling) such as the use of personal data to evaluate, analyse or predict an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
* any large-scale processing of special categories of personal data or criminal offence data;
* regular data sharing with a third party;
* any large-scale, systematic monitoring of a publicly accessible area.

**Individual rights**

Individuals have rights in relation to how we process their personal data, including the right to:

* receive the information contained in our privacy notices;
* withdraw their consent to processing at any time;
* request access to their personal data (known as a subject access request);
* ask us to stop us using their personal data for direct marketing purposes;
* ask us to erase their personal data if it is no longer necessary for the purpose it was collected;
* rectify inaccurate data or to complete incomplete data;
* restrict processing;
* object to processing on the basis of our legitimate interests;
* object to decisions based solely on automated processing, including profiling;
* receive or ask for their personal data to be transferred to a third party.

If someone makes a request to exercise one of these rights, or if you think someone may be trying to exercise one of these rights, you must inform maryanne.piggott@kcl.ac.uk or telephone 0207 848 8234 without delay. We will usually have one month in which to respond.

Unless you are authorised to do so, you should not attempt to respond to a request by an individual to exercise any of the rights listed above. Some of these rights only apply in certain situations and some may require the Society to take legal advice before responding.

You must not provide personal data to anyone in any circumstances without first verifying the identity of the individual making the request. Do not allow third parties to persuade you to disclose personal data without proper authorisation.

**Data Breach Procedure**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The following are examples of personal data breaches:

* access by an unauthorised third party (e.g. our systems are hacked);
* deliberate or accidental action (or inaction) by one of our suppliers which leads to our personal data being shared in an unauthorised way;
* sending an email containing personal data to an incorrect recipient;
* IT devices containing personal data being lost or stolen;
* loss of availability of personal data (e.g. our systems go down and we do not have information backed-up).

If you know or suspect that a personal data breach has occurred, you must contact maryanne.piggott@kcl.ac.uk or telephone 0207 848 8234 without delay. If they are unavailable, you should inform the President. You should not attempt to investigate the breach yourself.

We may ask you to provide more information to help us to investigate the breach. You should keep all evidence relating to the breach and, if possible, you should take any steps that might reverse or minimise the risks. This might include:

* recalling an email that was sent to the wrong person;
* asking someone to return a hard copy of a document they should not have received;
* seeking immediate IT support so that back-up copies of information can be recovered.

We keep a record of all personal data breaches. In certain circumstances, we must notify the Information Commissioner’s Office (ICO) and the individual about a personal data breach. All decisions about whether to make a report will be taken by the President and Secretary. The Anatomical Society may also report a breach as a serious incident to the Charity Commission.

*File: AS-Data-Protection-Policy:*

END