

FAS Data Protection Policy

Our data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.



The Federation of Astronomical Societies is committed to:

- ensuring that we comply with the data protection principles that are listed below
- meeting our legal obligations of the [Data Protection Act 1998](#)
- processing personal data only in order to meet operational needs or fulfil legal requirements
- establishing appropriate retention periods for personal data
- providing adequate security measures to protect personal data
- ensuring that a nominated officer (Data Controller) is responsible for data protection compliance
- ensuring that all nominated data processors are made aware of good practice in data protection
- ensuring that queries about data protection is dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines

Data protection principles

1. Personal data shall be collected, processed and used fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the [Data Protection Act 1998](#)
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The Federation of Astronomical Societies is registered. The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. To this end the designated officers will be responsible for notifying and updating the Data Controller of the processing of personal data, within their area. The Data Controller will review the Data Protection Register with designated officers annually, prior to notification to the Information Commissioner. Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between reviews should be brought to the attention of the Information Commissioner immediately.

Identification of FAS officers with data protection responsibilities:

Data Controllers: Webmaster; Membership Secretary; Handbook Editor

Data Processors: Newsletter distributor; Handbook Editor; Secretary; PLI Secretary

Data Collected

For our membership records and services to members purposes the FAS collects personal data from the contacts nominated by member societies to the FAS (typically the Secretary and Treasurer of each society).

We collect: contact name, address, e-mail address and telephone number for both contacts. In addition to this we collect information from each member society. We collect: name of society, number of members, e-mail address, website address, meeting location and typical meeting date. Most of this information is used for our own internal processing for membership and group PLI purposes (for those societies opting into the PLI scheme). Third party access is discussed below.

Third party access

We share basic contact details, so that interested members of the public may contact member societies, on our website and with the BBC Sky at Night Magazine. We do not share your personal data with any other organisation.

Security Procedures

We operate a data model such that only individual authorised users may access their own society data; this is via a password login system that is generated by the data controller. Data Controllers have access to the whole system via a different login. Access logs to the system are maintained. Data Processors are only given access to the required data and have no access to the overall system – this data is generated by the Data Controllers.

We undertake an annual risk assessment of our system to ensure that we minimise our exposure to data breaches and threats. In the event of a security breach we would ensure that our system was secured as soon as possible. We also would contact any concerned individuals and the Information Commissioner. We would then review how the security breach happened altering our system and/or providing new training procedures to try and prevent it happening again.