

**Data Protection Policy**

## Definitions

|  |  |
| --- | --- |
| **Association** | means The Association for Science Education (ASE), a registered charity number 313123, OSCR SC042473 and RC000805. |
| **GDPR** | means the General Data Protection Regulation under UK GDPR and the [Data Protection Act 2018](https://www.gov.uk/data-protection) (DPA 2018) and (GDPR) EU 2016/679 |
| **Responsible Person** | means the Chief Executive Officer, who will have responsibility for data protection within ASE. |
| **Register of Systems** | means a register of all systems or contexts in which personal data is processed by ASE. |
| **Data** | Information which relates to an identified or identifiable individual |
| **Data Controller** | ASE is the Data Controller. |
| **Data Protection Officer (DPO)** | The GDPR introduces a duty to appoint a DPO if you are a public authority, or if you carry out certain types of processing activities. ASE does not fall into any of these categories. |

### 1. Data protection principles

ASE has a duty to comply with UK law on data protection, which is governed by UK GDPR, tailored by the Data Protection Act 2018. It gives certain rights to individuals and it also says that those who record and use personal information must adhere to seven key data protection principles.

ASE is aData Controller as defined by UK GDPR, which means that it determines what data will be collected and for what purpose. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Article 5 of the UK GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

**These principles can be summarised as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.**

### 2. General provisions

1. This policy applies to all personal data processed by the Association.
2. The Responsible Person will take responsibility for ASE’s ongoing compliance with this policy.
3. ASEwill, through appropriate management, ensure that everyone processing personal data understands their responsibilities under UK GDPR and are appropriately trained and supervised.
4. This policy will be reviewed at least annually in conjunction with changes in law and guidance from the Information Commissioner’s Office (ICO).
5. ASE is registered with the ICO as an organisation that processes personal data.

### 3. Lawful, fair and transparent processing

1. ASE will identify a ‘lawful basis’ for all data processing – in most cases this is likely to be because clear consent has been obtained to process data for a specific purpose and / or the processing is necessary for a contract with an individual.
2. ASE will only handle personal data in ways people would reasonably expect.
3. ASE is committed to being transparent about how and why we use information. ‘Privacy information’ will be provided when data is collected in line with the ICO checklist. This will include the purposes the data is required for, the retention period and who the data will be shared with.
4. ASE will use appropriate systems and, as a small organisation, document processing activities that are not occasional (in practice this means data processing for membership and related services including CPD as well as for HR and recruitment).
5. The systems will be reviewed at least annually.
6. Individuals have the right to access their personal data and any such requests made to the Association will be dealt with within one month and using ICO guidance.
7. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the personal data.
8. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the ASE’s systems.

### 4. Purpose limitation

1. ASE will be clear why it is collecting personal data and what it intends to do with it and it will inform individuals about these purposes in its ‘Privacy information’.
2. If the purpose of holding information changes, new consent will be obtained.

### 5. Data minimisation

1. ASE will ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

### 6. Accuracy

1. ASE will take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps will be put in place to ensure that personal data is kept up-to-date.

### 7. Storage limitation

1. To ensure that personal data is kept for no longer than necessary, the Association will put in place an archiving policy for each area in which personal data is processed and review this process annually.
2. The archiving policy will consider what data should/must be retained, for how long, and why.
3. Data held will be reviewed every year and erased/anonymised when no longer needed.

### 8. Integrity and confidentiality

1. The Association will use appropriate cyber and organisational measures to ensure that personal data is stored securely and not accidentally or deliberately compromised. The level of security will take account of the assessed risks to the data and ASE’s size.
2. Access to personal data will be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions will be in place.
5. ASE will ensure that any data processor we use also implements appropriate technological and organisational measures to secure our information.

### 9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Association will promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)).

Last updated July 2023

END OF POLICY