AEGIS Data Protection Policy

Data Protection Statement

AEGIS (The Association for the Education and Guardianship of International Students) will comply with all statutory requirements of The Data Protection Act 1998 ("the Act") by taking all reasonable steps to ensure the accuracy and confidentiality of such information. AEGIS needs to gather and use certain information about individuals. These can be members, suppliers, business contacts, employees and other people the charity has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to the meet the AEGIS's data protection standards, and to comply with the legislation.

Why this policy exists:

This data protection policy ensures AEGIS:

- Complies with data protection law and follows good practice
- Protects the rights of staff, members and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of data breach.

The Information Commissioner's Office

The Information Commissioner's Office (ICO) is "*the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals*" (ICO website). It is responsible for administering the provisions of the Data Protection Act 1998; the Freedom of Information Act 2000 (not relevant to AEGIS); and the General Data Protection Regulation 2018.

The Act requires every data controller who is processing personal information to register with the ICO (unless exempt). AEGIS is registered with the ICO as a data controller, and this is renewed annually (Registration reference: Z2023128).

The ICO publishes a Register of data controllers on their website, on which AEGIS (The Association for the Education and Guardianship of International Students) is listed.

The Data Protection Act 1998

Directives lay down certain results that must be achieved but each Member State is free to decide how to transpose directives into national laws. EU directives are addressed to the member states, and are not legally binding for individuals in principle. The member states must transpose the directive into internal law – Acts. Directive 95/46/EC on the protection of personal data had to be transposed by the end of 1998, when it became now as *The Data Protection Act 1998.*

The Act protects individuals' rights concerning information about them held on computer and in any AEGIS personnel files and databases. These rules apply regardless of whether data is stored electronically, on paper or other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Freedom of Information Act 2000

The Freedom of Information Act 2000 provides public access to information held by public authorities, in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

General Data Protection Regulation 2018

Regulations have binding legal force throughout every Member State and enter into force on a set date in all the Member States. The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. When the GDPR takes effect, it will replace the 1995 Data Protection Directive (Directive 95/46/EC) - The Data Protection Act 1998. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance requires organisations to review their approach to governance and how they manage data protection as a corporate issue.

AEGIS will handle and protect all information in line with data protection principles set out in the Act. Under the Act, anyone processing data must comply with the eight principles of good practice for data protection, as detailed below:

Data will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive in relation to the purpose(s) for which they are processed
- Accurate and kept up to date
- Not kept longer than necessary
- Processed in accordance with the data subject's rights under the Act
- Secure and protected. Appropriate technical and organisational measures are in place to protect data from unauthorised or unlawful processing and from accidental loss, damage or destruction.
- Not be transferred to a country or territory outside of the European Economic Area (EEA) unless we can be assured there is an adequate level of protection for the rights and freedoms of the data subjects.

This AEGIS Data Protection policy applies to personal data as defined by the Act – that is, data from which a living individual can be identified, either from data alone, or from that data and other information that is held by the data controller. This includes information held on computer, paper files, photographs etc.

Responsibilities

This policy applies to the main office of AEGIS, all staff and volunteers of AEGIS, and all contractors and other people working on behalf of AEGIS. The scope of the policy applies to all data held by AEGIS relating to identifiable individuals. Everyone who works for AEGIS has responsibility for ensuring data is collected, stored and handled appropriately – all must ensure personal data is handled and processed in line with this policy and data protection principles.

The Board of Trustees is ultimately responsible for ensuring that AEGIS meets its legal obligations.

The data controller is responsible for:

- Keeping the Board of Trustees updated about data protection responsibilities, risks and issues – in the form of an annual report
- Reviewing all data protection procedures and policies
- Arranging data protection training if required
- Handling data protection queries from those working for and with AEGIS
- Dealing with requests from individuals relating to the data AEGIS holds about them
- Assisting with any agreements with third parties that may handle sensitive data
- Working with AEGIS's IT contractors to ensure that all systems, services and equipment used for storing data meet acceptable security standards, including ensuring regular checks, scans and updates to ensure security hardware and software are functioning properly.

The purpose of the Act is to make sure that personal data is used in a way that is fair to the individual and protects their rights, while enabling organisations to process personal data in pursuit of their legitimate aims.

Staff guidelines

- Personal data should not be shared informally – it should not be sent by email – this form of communication is not secure.
- Personal data must be encrypted before being transferred electronically. AEGIS uses an email server called 'Names.co.uk '. Transport Layer Security (TLS) is the protocol used by AegisUK's email system – a type of end-to-end encryption, which provides internet security over a computer network, which aims to privacy and data integrity between two communicating computer applications. AEGIS uses TLS to encrypt and protect email traffic in transit. Without the TLS, emails cannot be accessed by AEGIS. TLS is handled by the server and the software (for instance, Outlook). Webmail is the way to access AegisUK emails outside of Outlook or other email client/software. Only people with access details are

permitted to access the AegisUK webmail system. The webmail is password protected, and this needs to be a specific strength to work.

- Employees should not save copies of personal data to their own computers/laptops – personal data should always be accessed and updated via the central copy of any data – the AEGIS server.
- Employees should keep all data secure, taking sensible precautions and following these guidelines.
- Strong passwords must be used, and never shared.
- Personal data should not be disclosed to unauthorised people, either within AEGIS or externally.
- Data should be regularly reviewed and updated if found to be out of date. If no longer required, it should be deleted and/or disposed of.
- When not in use, paper format data or files (for instance, DBS applications) should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for instance, on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When working with personal data, employees should ensure computer/laptop screens are always locked when left unattended.
- Where date is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- If data is stored on removable media (for instance, a CD or USB), these should be kept looked away securely when not in use.
- Data should only be stored on designated drives and servers, and/or approved cloud computing services.
- Data should be backed up frequently, and backups should be tested regularly.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Personal data should never be saved directly to laptops or other mobile devices like smart phones or tablets, unless encrypted.

AEGIS may collect and process the following examples of data:

- Full name (including title, forename(s), family name)
- Job title
- Contact information (for example, current home/business address, telephone numbers, email addresses, website address)
- Qualifications/experience
- Date of birth
- Information relevant to HR (for example: C.V.s, interview notes, referee details)
- DBS reference number
- Full name of Guardianship Organisation (GO) and personnel
- Details required for AEGIS Annual Declaration (for example: dates of formation of GO, GO registration number & date, details of local co-ordinators, AEGIS Inspection and re-inspection dates, details of Professional Indemnity and Public Liability Insurance, overseas student numbers and type of schooling, total number of homestays, total number of students, details of safeguarding training)
- School name and personnel

- School year group
- Main language for correspondence
- Level of guardianship service provided
- Date of last visit for student (at homestay)
- Whether private fostering assessment has been undertaken by the Local Authority
- Details of venues (name, location, address, contact details)
- Feedback forms
- Photographs (for example, students, guardians, inspectors)

AEGIS may use/process this information to:

- Contact parents, homestays and schools
- Undertake administrative functions (for example, HR, contact referees)
- Process DBS applications (act as counter signatory)
- Compile marketing lists (e.g. for newsletter and conferences)
- Handle complaints
- Conduct research
- Share anonymous details with 3rd parties for the purpose of obtaining professional advice
- Understand people's views and opinions (for example, via feedback forms)
- Send out information that AEGIS thinks might be of interest to others
- Improve our services
- Comply with legal and regulatory obligations

Protecting your information

AEGIS has appropriate technical and organisational measures in place to protect your information. Paper files are locked away securely and electronic files are protected by access rights (strong passwords are used) set at a server level. All electronic files are backed up every workday (excluding weekends), using AES 256 password strength encryption. AEGIS's server cannot be remotely accessed, and is only accessible in the office and when connected to the internet/networks, using log in details.

Data accuracy

The law requires AEGIS to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees and people working with AEGIS, who work with data, to take reasonable steps to ensure it is kept accurate and as up to date at possible.

- Data should be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated, for instance, details can be updated when a member calls.
- AEGIS will make it easy for data subjects (for instance, guardianship organisations and school members) to update their own information AEGIS holds about them, for instance, via the AEGIS website.

- Any data inaccuracies should be corrected as soon as discovered, for instance if a member can no longer be reached on their stored telephone number, this should be removed from the database).

Data protection risks

This policy helps to protect AEGIS from data security risks including:

- Breaches of confidentiality, for instance: information being given out inappropriately
- Failing to offer choice, for instance: all individuals should be free to choose how the company uses data relating to them
- Reputational damage, for instance: the company could suffer if hackers successfully gained access to sensitive data.

Accessing your information

Under the Act, an individual is entitled to ask AEGIS:

- For a copy of the personal information held by AEGIS
- For any inaccuracies to be corrected
- How to gain access to such data
- How they are meeting their data protection obligations

Such requests are known as 'Subject access requests'. Such requests should be made either via email or via the post.

Email requests should be addressed to the data controller at info@aegisuk.net.

Postal requests should be submitted to: AEGIS, Data Controller, The Wheelhouse, Bond's Mill Estate, Bristol Road, Stonehouse, Gloucestershire GL10 3RF.

There is no administration charge for any subject access request. The data controller will aim to provide the relevant data within 14 working days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Sharing your personal information

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, AEGIS will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board of Trustees, and by taking legal advice where necessary.

If on the rare occasion, we need to share data, we will only use data anonymously.

If personal information is shared, it will be done so in line with the Act. You are entitled to know why and how we are sharing your personal information and the organisation or individual receiving your personal information will be required to protect your information in line with the Act.

Logging and recording of communications with individuals

AEGIS may log communications with you for the purposes described earlier in this policy.

Links to other websites on the AEGIS website

Our website includes links to other websites (for example: to other organisations dealing with boarding students, government departments and agencies). We are not responsible for the data protection and privacy practices of these organisations, including their website. This Data Protection Policy applies to AEGIS only.

Cookies

Refer to AEGIS Privacy Notice on the AEGIS website.

Providing information

AEGIS aims to ensure that individuals are aware that their data is being processed, and that they understanding:

- How the data is being used
- How to exercise their rights

To these ends, a copy of this policy which sets out how data relating to individuals is used by AEGIS can be available on request. This policy is also available on the AEGIS website.

For further information

If you have any questions about this policy, please contact the Data Controller at AEGIS via email at info@aegisuk.net or by post at: AEGIS, Data Controller, The Wheelhouse, Bond's Mill Estate, Bristol Road, Stonehouse, Gloucestershire GL10 3RF.

Policy prepared by:	Elaine Austin – Administration Assistant
Approved by Board of Trustees:	23rd May 2018
Policy became operational on:	23rd May 2018
Next review date:	May 2019