AEGIS Data Protection Policy

January 2025

AEGIS Data Protection Policy

1. Introduction and Purpose

This policy outlines our approach to handling personal information in accordance with the UK General Data Protection Regulation 2016 and the Data Protection Act 2018.

For the purposes of this policy, AEGIS is the data controller, and we are registered with the Information Commissioner's Office (ICO) under registration number is Z2023128.

The purpose of this Policy is to explain how we handle personal information under the relevant data protection laws, and to inform employees and other individuals who process personal information on our behalf, of our expectations in relation to this.

2. Scope

This policy applies to the processing of personal information that is held by AEGIS. This includes personal information about employees, volunteers, temporary staff, contractors, members, visitors, and any other individuals who engage with us.

This policy should be read in conjunction with the AEGIS Privacy Policy.

3. Definitions

The following terms are used throughout this policy, and it is important that you understand what they mean:

- Personal data: Any information relating to a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- Data subject: the identified or identifiable living individual to whom personal data relates.
- Controller: A person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- Processor: A person or organisation which processes personal data on behalf of the controller, and in accordance with their instructions.
- Processing: This is anything that you do with data, including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.

- Special category data: This is personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes genetic data, biometric data, and data concerning a person's health, their sex life, and sexual orientation.

4. Roles and Responsibilities

AEGIS is the data controller, and we are responsible for complying with the UK GDPR.

Board of Trustees

The Board of Trustees has overall responsibility for ensuring that this policy is implemented.

Chief Executive Officer (CEO)

The Chief Executive Officer has day-to-day responsibility for ensuring that this policy is adopted and adhered to by employees and all other individuals who process personal information on behalf of AEGIS.

Employees, Temporary Staff, Contracts and Visitors

All employees, temporary staff, contractors, visitors, and any other individuals who process personal information on behalf of AEGIS, are responsible for complying with this policy in its entirety.

Failure to comply with this policy may result in disciplinary action being taken, or the termination of an employment or service contract.

5. Data Protection Principles

The UK GDPR sets out several key principles which govern how AEGIS handles personal information. Complying with these principles helps us to ensure that we comply with the law, and that our practices in relation to data protection are good.

The principles state that personal information must be:

- Processed in a way that is lawful, fair, and transparent ("lawfulness, fairness, and transparency).
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation").
- Adequate, relevant, and limited to what is necessary ("data minimisation").
- Accurate, and where necessary, kept up to date ("accuracy").

- Kept for no longer than is necessary ("storage limitation").

- Processed in a way that ensures it is safe and secure, by means of appropriate technical and organisational measures ("integrity and confidentiality").

The UK GDPR requires us to be able to evidence that we are complying with these principles. This is called the "accountability principle".

Lawfulness, Fairness and Transparency

We only process personal information where there is a lawful basis for doing so. The lawful bases are as follows:

- Where the data subject has given us their consent to the processing.

- Where processing is necessary for the performance of a contract, or to enter into a contract, with the data subject.

- Where processing is necessary to comply with a legal obligation that we are subject to.

- Where processing is necessary to protect the vital interests of the data subject or another person.

- Where processing is necessary for the performance of a task carried out in the public interest.

- Where processing is necessary for the purposes of the legitimate interests pursued by AEGIS or by a third party, except where such rights are overridden by the interests or fundamental rights and freedoms of the data subject.

We will only process special category data where a lawful basis has been identified from the list above, plus one from the following list:

- The data subject has given us their explicit consent.

- The processing is necessary for the purposes of exercising or performing any right or obligation which is imposed on AEGIS in relation to employment, social security, and social protection law.

- The processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving consent.

- The processing is necessary for the establishment, exercise, or defence of legal claims.

- The processing is necessary for reasons of substantial public interest.

- The processing is necessary for preventative or occupational medicine, medical diagnosis, the assessment of the working capacity of an employee, or for the provision of health and social care treatment.

The principle of fairness means that personal information should be used in a way that the data subject would reasonably expect.

The UK GDPR defines 'consent' as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

When we rely on consent as the basis for processing personal information, we will ensure that the data subject is able to withdraw their consent as easily as they gave it, and at any time.

We will always use the most appropriate basis for processing personal information.

The principle of transparency requires AEGIS to ensure that any information provided by us to data subjects about how their personal information will be processed, is concise, easily accessible, easy to understand, and written in plain language.

Purpose Limitation

We will be clear from the very beginning as to why we are collecting personal information and what we intend to do with it.

We will only collect personal information for specified, explicit, and legitimate purposes, and we will not process information in any way that is incompatible with those purposes.

If things change, and we intend to use personal information for a different purpose, we will make sure that the new use is fair, lawful, and transparent. We will always inform data subjects before we use their personal information for a new purpose, and where the lawful basis relied upon for the original purpose was consent, we will obtain such consent again.

Data Minimisation

The personal information that AEGIS collects and processes will be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

Accuracy

The personal information that AEGIS collects and processes will be accurate and, where necessary, kept up to date, and will be corrected or deleted without delay when we are notified that the information is inaccurate.

AEGIS employees are required to update all relevant records if they become aware that any personal information is inaccurate.

Storage Limitation

We do not keep personal information for longer than we need it.

We carefully consider how long we keep personal information for, and we justify our reasons for keeping it. Most of our retention periods are determined by legal timescales. For example, personal information relating to income tax contributions.

We have a retention schedule in place which details the types of personal information we hold, the reasons for holding it, and the retention period. This schedule forms part of our Record of processing activities (please see Section 12: Record of Processing Activities).

We regularly review the data we hold and delete or securely destroy it when we no longer need it.

Integrity and Confidentiality

We take our responsibilities under data protection laws very seriously and we will always ensure that we have appropriate security measures in place to protect the personal information we hold.

This means that we will have appropriate measures in place to protect personal information against unauthorised or unlawful processing, accidental loss, destruction, or damage.

AEGIS employees are responsible for ensuring the security of the personal information processed by them in the performance of their duties and tasks.

6. Keeping Personal Information Secure

We have appropriate technical and organisational measures in place to ensure that we process personal information securely, and to prevent personal information we hold being accidentally or deliberately compromised.

Technical Measures

- We enforce strong password policies; passwords are changed at appropriate intervals and are not shared or used by others.
- We ensure that laptops, USB/memory sticks and other portable devices containing personal information are encrypted.
- We have a firewall, anti-virus, and anti-malware software in place.

- We restrict access to systems, so personal information is only accessible to those people who need to use it as part of their work.

- Paper documents containing personal information are securely destroyed using a shredder when they are no longer required.

Organisational Measures

- We have appropriate policies and procedures in place to ensure our employees fully understand their responsibilities under data protection laws.

- We ensure that our employees and any other individuals who process personal information on behalf of AEGIS, are aware of their individual responsibilities under data protection laws and how these apply to their areas of work.

- We promptly investigate all suspected personal data breaches; we always make the appropriate external notifications (where applicable) and seek to learn any lessons from the incident to reduce the risk of reoccurrence.

- Paper documents containing personal information are securely locked away when not in use.

- Paper documents containing personal information are securely destroyed using shredders when they are no longer needed.

- Employees take every opportunity to ensure that the personal information we hold is accurate and kept up to date.

- Employees do not disclose personal information to any unauthorised persons, both externally and within AEGIS.

We regularly test, assess, and evaluate the effectiveness of the measures we have put in place, and act on the results of those tests where they highlight areas for improvement.

7. Managing Personal Data Breaches

We have a procedure in place for managing and responding to personal data breaches.

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

Examples are personal data breaches include:

- Sending personal data to the wrong person.
- Access to personal data by an unauthorised third party.
- Devices or equipment containing personal data being lost or stolen.

All suspected personal data breaches and security incidents must be reported without delay to the CEO. All personal data breaches will be investigated promptly and recorded on our internal data breach register.

The CEO is responsible for deciding whether a personal data breach needs to be reported to the ICO and data subjects.

Notifying the ICO and Other External Authorities

Where a personal data breach is likely to result in a risk to the rights and freedoms of a data subject(s), AEGIS will notify the ICO within 72 hours of becoming aware of the breach.

We may be required to notify a personal data breach to other external authorities. For example, we may be required to notify the Charity Commission. The CEO is responsible for agreeing all external notifications.

Notifying Data Subjects

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject(s), AEGIS will communicate the personal data breach to the data subject(s) without undue delay.

When informing the data subject(s) about the breach, AEGIS will provide in clear, plain language, the following information:

- Details about the nature of the breach.
- The name and contact details of the organisational point of contact, who the data subject(s) can contact if they require further information.
- The likely consequences of the breach.
- Measures taken, or proposed to be taken, to address the breach including measures mitigate possible adverse effects.

8. Responding to Requests from Individuals ("Rights of Data Subjects")

The UK GDPR provides data subjects with a number of rights in relation to their personal information.

These are:

- The right to request a copy of the personal information we hold about them.
- The right to request that inaccurate or incomplete information about them is rectified.

- The right to request that their personal information is deleted.
- The right to request that the processing of their personal information is restricted.
- The right to data portability.
- The right to object to the processing of their information.
- The right to complain to the ICO if they are not happy with how their personal information has been processed, or they feel their data protection rights have been infringed.

We will endeavour to respond to all requests without delay, and in any event within one month of receiving a request. There may be circumstances when we need to extend the time limit for responding to a request. We will tell the individual who has made the request if this is the case and keep them informed.

Before responding to a request, we may need to ask for further information and/or proof of the individual's identity.

There may be exceptions to the rights outlined above; each request we receive will be reviewed on a case-by-case basis.

9. Document Retention

We do not keep personal information for longer than we need it.

We carefully consider how long we keep personal information for, and we justify our reasons for keeping it. Most of our retention periods are determined by legal timescales. For example, personal information relating to income tax contributions.

We have a retention schedule in place which details the types of personal information we hold, the reasons for holding it, and the retention period. This schedule forms part of our Record of processing activities (please see Section 12: Record of Processing Activities).

We regularly review the data we hold and delete or securely destroy it when we no longer need it.

10. Data Protection by Design and Default

We consider data protection and privacy issues upfront in everything we do. We are required to do this under the UK GDPR.

We make sure that when we are designing and implementing a new organisational system, service, or practice, we consider the data protection issues before we begin. We also make sure, by default, that we only process personal information where it is necessary to do so.

11. Data Processors

Whenever we use a third party to process personal information on our behalf, we will always undertake appropriate due diligence and ensure a data processing agreement is in place.

We only use processors that provide us with sufficient guarantees about their security measures.

12. Record of Processing Activities

AEGIS maintains a record of its processing activities, as is required under Article 30 of the UK GDPR. This record is held in electronic format and contains the following information:

- Our organisation name and contact details.
- A description of the personal information we process.
- Categories of data subjects.
- Purposes of the processing.
- Recipients of the personal information.
- The name of any countries or organisations outside the UK that we transfer personal information to, together with information about the safeguards in place.
- Retention periods.
- A general description of our technical and organisational security measures e.g., encryption, access controls, and training.

We regularly review the personal information we process and update this record accordingly. This record will be made available to the ICO, if requested.

13. Data Protection Impact Assessments (DPIA's)

A Data Protection Impact Assessment (DPIA) is a process that helps us to identify and minimise the data protection risks associated with a project, process, or activity involving the processing of personal information.

We are required to carry out a DPIA for any processing that is likely to result in a high risk to individuals. We will also carry out a DPIA for any other major project which requires the processing of personal information, because it is good practice to do so.

The DPIA will:

- Describe the nature, scope, context, and purposes of processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

We will record the outcome of the DPIA and implement the measures identified.

14. Appointment of a Data Protection Officer

Under Article 37 of the UK GDPR, controllers and processors are required to appoint a Data Protection Officer if:

- The processing is carried out by a public authority or body.
- The core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of individuals on a large scale.
- The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

The status of our organisation (AEGIS is not a public body) and the scope of our processing activities means that we are not required to appoint a Data Protection Officer.

We will keep this decision under review, should our processing activities change.

15. Policy Review

This policy was last updated in January 2025.

We will review this policy on an annual basis, or when there is a change to data protection laws or our organisational policies and procedures.

Contact Details

Chief Executive Officer Yasemin Wigglesworth yasemin@aegisuk.net
Chair of the Trustees Edward May edward@aegisuk.net