

# Elysian

## Data Protection / GDPR Policy



**Date Agreed: April 2024**

**Date of next review: April 2025**

Page Break

***Elysian is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.***

This policy applies to all sites on which Elysian operates.

### **POLICY STATEMENT**

This is the Data Protection Policy of Elysian Animal Assisted Interventions Ltd, hereafter referred to as 'Elysian'.

We are committed to processing Personal Information fairly and lawfully in accordance with the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 ("The DPA") and other related legislation which protects Personal Information. We recognise the importance of this and have updated our Policy to ensure that it gives effect to these important changes in the law.

As a School, it is necessary for us to process Personal Information about our staff, learners, parent(s) / guardian(s) and other individuals who we may come into contact with. In doing so, we recognise that the correct and lawful treatment of Personal Information is critical to maintaining the confidence of those connected with Elysian.

This Policy has been updated to reflect our ongoing commitment to promoting a strong culture of data protection compliance in accordance with the law.

## **ABOUT THIS POLICY**

This Policy, and any other documents referred to in it, sets out our approach to ensuring that we comply with data protection laws. It is critical that staff and governors understand their responsibilities to handle Personal Information in accordance with the law and support Elysian in meeting its aim of maintaining a strong data protection culture.

This Policy does not form part of any employee's contract of employment and may be amended at any time.

This Policy has been approved by the Governing Body.

## **DEFINITION OF DATA PROTECTION TERMS**

We have set out below some of the terms used in this policy along with a brief explanation about what they mean.

**Data Subjects** means an identified or identifiable natural person. For example, we process personal information about parents, staff members and learners, each of whom is a data subject.

**Personal Information** means any information about a data subject. Examples of personal information could include information about a learner's attendance, medical conditions, Special Educational Needs requirements or photographs.

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identify. Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

**Privacy Notices** are documents provided to data subjects which explain, in simple language, what information we collect about them, why we collect it and why it is lawful to do so. They also provide other important information which we are required to provide under data protection laws.

**Data Controllers** determine the purpose and means of processing personal information. They are responsible for establishing practices and policies in line with the GDPR. Elysian is a 'Data Controller'.

**Data Users** are those of our staff members whose work involves processing personal information. Data users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

**Processing** means when personal information is used in a particular way. For example, we may need to collect, record, organise, structure, store, adapt or delete personal information. When we do this, we will be 'Processing'.

**Special Category of Personal Information** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, data concerning a data subject's sex life or sexual orientation. These types of personal information are regarded as being more 'sensitive' and the law requires increased safeguards to be in place if we are to process this type of data.

## **DATA PROTECTION PRINCIPLES**

When we Process Personal Information, we will do so in accordance with the 'data protection principles. In this regard, we will ensure that Personal Information is: -

1. Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
2. Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).
4. Accurate and where necessary kept up to date (**Accuracy**).
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data 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 (**Security, Integrity and Confidentiality**).

We recognise that not only must we comply with the data protection principles, but we must also demonstrate our compliance with these principles (**Accountability**).

## **DATA PROTECTION OFFICER**

Our appointed DPO is Jo Nunn. Jo can be contacted on 07944 875155 or [admin@elysianuk.org](mailto:admin@elysianuk.org)

The DPO will carry out a number of important tasks which will include: -

1. monitoring compliance with data protection laws and our data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits.
2. advising on, and monitoring, data protection impact assessments.
3. cooperating and being the first point of contact with the Information Commissioner's Office, members of staff, parents and learners.

## **LAWFULNESS, FAIRNESS, TRANSPARENCY**

### **Lawful Processing**

Personal Information must be Processed lawfully. Under data protection laws, there are a number of grounds which make it lawful to Process Personal Information. We will only Process Personal Information if one or more of the following apply: -

1. the Data Subject has given his, her or their **consent**.
2. the Processing is necessary for the **performance of a contract** with the Data Subject.
3. the Processing is necessary to meet our **legal obligations**.
4. the Processing is necessary to protect the Data Subject's **vital interests**.
5. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (often referred to as **Public Task**).

We recognise that some categories of Personal Information are more sensitive and further conditions must be satisfied if we are to Process this information (Special category and criminal conviction data). Where we Process these categories of Personal Information, we will ensure that we do so in accordance with the additional conditions for Processing set out under the GDPR and the DPA.

## Consent

Where it is necessary for us to obtain consent to process Personal Information, we will ensure that we do so in accordance with data protection laws.

Generally, we will only obtain consent where there is not another lawful ground (see 6.1) for Processing. Some examples as to when we will obtain your consent is if we want to place a photograph of a learner in the newspaper, on social media or in other publications to celebrate their achievements.

We recognise that under data protection laws, there are stricter rules as to how consent is obtained. We will ensure that when we obtain consent, we: -

1. take steps to ensure that we make it clear to Data Subjects what they are being asked to consent to.
2. ensure that the Data Subject, either by a statement or positive action, gives their consent. We will never assume that consent has been given simply because a Data Subject has not responded to a request for consent.
3. never use pre-ticked boxes as a means of obtaining consent.
4. ensure that a Data Subject is informed that they can withdraw their consent at any time and the means of doing so.
5. keep appropriate records evidencing the consents we hold.

## Commitment

The school is committed to always maintaining the principles and duties in the GDPR. Therefore, the school will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer.
- Inform individuals of the purposes that personal information is being collected and the basis for this.
- Inform individuals when their information is shared, and why and with whom unless GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up to that point.
- Provide details of the length of time an individual's data will be kept.
- Should the school decide to use an individual's personal data for different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests).

- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

## **Transparency**

We are required to provide information to Data Subjects which sets out how we use their Personal Information as well as other information required by law. We will provide this information by issuing Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear, plain language.

## **PROCESSING FOR LIMITED PURPOSES**

We will only collect and Process Personal Information for specified explicit and legitimate reasons. We will not further Process Personal Information unless the reason for doing so is compatible with the purpose or purposes for which it was originally collected.

## **ADEQUATE, RELEVANT AND LIMITED PROCESSING**

We will only collect Personal Information to the extent that it is necessary for the specific purpose notified to the Data Subject.

## **ACCURATE DATA**

We will ensure that Personal Information we hold is accurate and kept up to date.

We will take all reasonable steps to ensure that Personal Information that is inaccurate is either erased or rectified without delay.

In supporting Elysian to maintain accurate records, staff, parents and other individuals whose Personal Information we may Process are responsible for: -

1. Checking that any information that they provide to the education provision is accurate and up to date; and
2. Informing the education provision of any changes to information that they have provided.

## **RETENTION**

We will not keep Personal Information for longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy and erase from our systems, all data which is no longer required.

We will maintain a records retention schedule which will assist the education provision to destroy Personal Information once it is no longer necessary and in a safe and secure manner.

## **INDIVIDUAL RIGHTS**

We will Process all Personal Information in line with a Data Subject's rights, in particular, their right to:

1. Request **access** to any data held about them by Elysian.
2. **Rectification** of inaccurate information.
3. **Erase** of Personal Information.
4. **Restrict** the Processing of Personal Information.
5. **Object** to the Processing of Personal Information.

6. To receive Personal Information in a commonly used format (known as **data portability**) and have this transferred to another controller without hindrance.

We will maintain a clear procedure detailing how such requests will be handled.

## **DATA SECURITY**

We will implement appropriate technical and organisational measures to guard against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources and the level of risk identified.

## **PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS**

We will integrate privacy by design measures when Processing Personal Information by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

We will utilise Data Protection Impact Assessments ("DPIAs") which will be used when introducing new technologies or the Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

## **ACCOUNTABILITY**

As a Data Controller, we are responsible for, and must be able to demonstrate, compliance with the data protection principles. Examples of how we will demonstrate compliance include (but are not limited to): -

1. appointing a suitably qualified DPO.
2. implementing policies and procedures e.g., a data protection policy, data breach procedures and subject access procedures.
3. undertaking information audits and maintaining a record of our processing activities in accordance with Article 30 of the GDPR.
4. preparing and communicating Privacy Notices to Data Subjects.
5. providing appropriate training at regular intervals.
6. implementing privacy by design when Processing Personal Information and completing data protection impact assessments where Processing presents a high risk to the rights and freedoms of Data Subjects.

## **DISCLOSURE AND SHARING OF PERSONAL INFORMATION**

Where it is necessary to share Personal Information outside of the education provision, we will inform you about this in accordance with this policy.

Examples of who we may share Personal Information with include other schools, the Local Authority and the Department of Education.

## **DATA BREACHES**

All data breaches must be handled in accordance with the education provision internal breach reporting procedure.

This policy will be reviewed annually by the Head of Education and Learning, in conjunction with the Chair of Governors, to ensure it is up to date with the latest developments in GDPR.

April 2024

For the purposes of this policy, where the term Elysian is used, it refers to Elysian Animal Assisted Interventions Ltd including Elysian School and Elysian Assisted Therapy & Learning.