Elysian
Data Protection / GDPR Policy

Date Agreed: June 2026
Date of next review: June 2027

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

POLICY STATEMENT

This is the Data Protection Policy of Elysian Animal Assisted Interventions Ltd, Elysian Training and Development Ltd and Elysian Animal Assisted Therapy and Learning C.I.C, all 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.

This policy also reflects updates introduced under the Data (Use and Access) Act 2025, which supplements UK GDPR and the Data Protection Act 2018. These updates include changes to subject access request handling, requirements for appropriate and proportionate searches, clarification processes, and strengthened expectations regarding complaints handling and accountability.

As an organisation, 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, set 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

- **Data Subjects:** Identified or identifiable natural persons, such as parents, staff members, and learners.
- **Personal Information:** Any information about a Data Subject, including attendance records, medical conditions, and photographs.
- **Privacy Notices:** Documents provided to Data Subjects explaining what information is collected, why, and the legal basis for processing.
- **Data Controllers:** Determine the purpose and means of processing personal information. Elysian is a 'Data Controller'.
- **Data Users:** Staff members whose work involves processing personal information. They must protect the data in accordance with this Policy and any applicable data security procedures.

- **Processing:** Actions involving personal information, such as collecting, recording, organising, storing, or deleting.
- **Special Category of Personal Information:** Sensitive data requiring increased safeguards, such as racial or ethnic origin, political opinions, or health data.

DATA PROTECTION PRINCIPLES

When we Process Personal Information, we will do so in accordance with the data protection principles:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected only for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Not kept in a form permitting identification longer than necessary.
6. Processed in a manner ensuring security using appropriate technical and organisational measures.

We recognise that we must not only comply with these principles but also demonstrate our compliance.

DATA PROTECTION OFFICER

Our appointed DPO is Jo Nunn. Jo can be contacted at 07944 875155 or admin@elysianuk.org.

The DPO's responsibilities include:

1. Monitoring compliance with data protection laws and policies.
2. Conducting internal audits and providing training.
3. Advising on data protection impact assessments.
4. Being the first point of contact with the ICO, staff, parents, and learners.

LAWFULNESS, FAIRNESS, TRANSPARENCY

Personal Information must be Processed lawfully. We will only Process Personal Information if one or more of the following apply:

1. The Data Subject has given consent.
2. The Processing is necessary for a contract with the Data Subject.
3. The Processing is necessary to meet legal obligations.
4. The Processing is necessary to protect the Data Subject's vital interests.
5. The Processing is necessary for a task in the public interest or the exercise of official authority.

For Special Category data, additional conditions apply.

For Special Category data, additional conditions apply.

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.

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 sets out how long different categories of data will be retained. This schedule is reviewed regularly to ensure compliance with legal and regulatory requirements.

All staff must adhere to the retention schedule and ensure that records are disposed of securely when no longer required.

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. Erasure 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.

SUBJECT ACCESS REQUESTS (SARs)

We will respond to Subject Access Requests in accordance with UK GDPR and the Data (Use and Access) Act 2025.

We will:

• respond within one month of receipt of a valid request, or up to 3 months where a request is

• verify the identity of the requester before processing

• request clarification where a request is unclear or broad (the statutory timeframe may be paused until clarification is received)

• conduct searches that are reasonable and proportionate to the nature of the request

• apply appropriate exemptions and redactions where required

We will maintain clear internal procedures to ensure that requests are handled consistently and in line with current ICO guidance.

DATA PROTECTION COMPLAINTS

Individuals have the right to raise a concern or complaint about how their Personal Information is processed. Complaints should be made in writing to the Data Protection Officer. All complaints will be acknowledged and investigated within a reasonable timeframe.

We will:

• record all complaints received

• investigate fairly and proportionately

• provide a response outlining findings and any actions taken

If an individual is not satisfied with our response, they have the right to escalate their complaint to the Information Commissioner's Office (ICO).

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.

CCTV AND VIDEO RECORDING

Where CCTV or video recording systems are in use, we will ensure that they are operated in compliance with data protection law.

This includes:

• having a clear lawful basis for processing

• ensuring appropriate signage is in place

• limiting access to recordings to authorised personnel only

• retaining recordings only for as long as necessary

• ensuring recordings are stored securely

The use of recording devices by staff will be strictly controlled and must be authorised in advance. This includes the use of mobile devices.

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.

USE OF ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

Where new technologies, including artificial intelligence (AI), are used to process Personal Information, we will ensure that appropriate safeguards are in place.

We will:

• complete a Data Protection Impact Assessment (DPIA) prior to implementation where required

• ensure transparency regarding how Personal Information is used

• avoid entering Personal Information into AI systems unless appropriate safeguards and agreements are in place

• ensure that meaningful human oversight is maintained in decision-making processes

Use of such technologies will be regularly reviewed to ensure continued compliance with data protection legislation and guidance.

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.

Senior leadership and governors have overall responsibility for ensuring that the organisation meets its data protection obligations.

All staff are responsible for:

• handling Personal Information in accordance with this policy

• reporting concerns or breaches promptly

• completing required training

All staff will receive data protection training as part of their induction, with regular refresher training provided. Additional training will be provided where roles require more detailed knowledge, such as handling Subject Access Requests or safeguarding information.

The Data Protection Officer provides oversight, advice, and monitoring of compliance.

DISCLOSURE AND SHARING OF PERSONAL INFORMATION

Where it is necessary to share Personal Information outside of the organisation, we will inform you about this in accordance with this policy. Examples of who we may share Personal Information with includes other schools, the Local Authority and the Department of Education.

SAFEGUARDING AND INFORMATION SHARING

We recognise that data protection legislation does not prevent the sharing of information where this is necessary to safeguard children or individuals at risk.

Where safeguarding concerns arise:

• we will share information lawfully, fairly and proportionately

• we will not rely on consent where it is not appropriate to do so

• we will consider the safety and welfare of the individual as the primary concern

• we will record decisions and the rationale for sharing information

All staff will follow safeguarding guidance alongside data protection requirements when making decisions about information sharing.

COMMUNICATION WITH FORMER EMPLOYEES

Once an individual's employment with Elysian has ended, they must no longer be given access to or receive any Personal Information or confidential data relating to learners, staff, or other stakeholders. This includes sensitive or special category data. Any inadvertent sharing of such information with ex-employees must be treated as a data breach and reported in line with our internal procedures.

DATA BREACHES

All data breaches must be reported immediately in accordance with the organisation's internal breach reporting procedure.

We will:

• investigate all breaches promptly

• take appropriate action to mitigate risk

• maintain a record of all breaches, regardless of severity

Where a breach presents a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner's Office (ICO) within 72 hours, in line with legal requirements.

INTERNATIONAL DATA TRANSFERS

Where Personal Information is transferred outside of the United Kingdom, we will ensure that appropriate safeguards are in place to protect the data.

This may include:

• transfers to countries deemed adequate by the UK government

• use of approved contractual clauses

• ensuring equivalent levels of data protection

All such transfers will comply with UK GDPR requirements.

This policy will be reviewed annually by the Strategic Lead for Compliance and Quality Assurance & DPO, to ensure it is up to date with the latest developments in GDPR.