DATA PROTECTION POLICY

2017-2018

Statement:

This policy document outlines the compliance of the company with GDPR for the protection of data processed as part of the company's ongoing activities in relation to the provision of alternative educational placements, and the processing of personal data related to students, staff and professional.
In this respect the protection of data, in particular sensitive data will be given the same status as safeguarding as in some circumstances a data breach can impact the safety of staff and students in a number of ways.

CONTENT:

- 8 principles of data protection and processing
- Policies
- Glossary
- Table of Lawful bases
- Table of Subject rights
- Exemptions to subject rights in relation to lawful bases
- Retention schedules (brief)
- Data protection impact assessment (brief)
- Types of data covered by GDPR
- GLOSSARY of TERMS

GLAS Ltd data protection and processing procedures follow from the 8 Data Protection Principles outlined below; -

First principle	Data must be processed lawfully, fairly and in a transparent manner in relation to individuals;
Second Principle	Data must be 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 shall not be considered to be incompatible with the initial purposes;
Third principle	Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
Fourth principle	Data must be 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;
Fifth Principle	Data must be 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
Sixth Principle	Personal information must be processed within the rights of the data subject.
Seventh Principle	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."
Eight Principle	Data must not be transferred internationally without adequate protection

Policies: -

All data collected and processed by GLAS Ltd in the capacity of 'Controller' are subject to the following policies: -

It is the company policy of GLAS Ltd to comply with the General Data Protection Regulation which includes: -

- All data must be included in our Information Asset Register prior to its collection and processing which includes the following features: -
    - The type of data (personal or special category)
    - The reason for collection and processing the data
    - At least one lawful basis for collecting and processing the data (see 'lawful basis' below)
    - Justification for the lawful basis selected
    - Whether the organisation processing is a controller or a processor (or both)
    - Retention schedules
    - Whether the data will be shared with another person or organisation and who that person or organisation is.
    - When the data is deemed to be special category data (see below for details of what constitutes special category data) further justification must be added to the register.
    - The level of risk to the data subject should the data suffer a breach of security
- When data is to be shared, an information sharing agreement must be in place
- Data may only be shared with persons or organisations that have been included in the privacy statement.
- When further processing or sharing which is not already outlined in the information asset register, information sharing agreement and privacy agreement is deemed necessary, the information asset register, information sharing agreement and the privacy notice must be updated.
- all data subjects must be issued with a privacy notice containing the following information: -
    - Why the data is collected
    - Why the data is processed
    - The lawful basis for collecting and processing the data

    - Justification for the lawful basis for collecting and processing the data
    - Who (persons or organisations) if anyone, the data will be shared with and why
    - How long the data will be kept for (retention schedules)
    - The data subject's rights under the General Data Protection Regulations and how to apply them.
    - How to complain and who to complaint to, if they think the data is being collected or processed in contravention of the general Data Protection Regulations
- The rights of data subjects relevant to the lawful bases outlined under the GDPR must be complied with at all times and within specified timeframes. (not all rights are applicable to all lawful bases – see below for exemption)
- All applications of subject rights will be subject to the processes outlined in the GLAS Ltd Subject Rights Procedure and Guidance document.
- Subject access requests must be completed within 30 days of the request being made unless an extension is deemed appropriate in special circumstances in which a further 2 months can be applied.
- Subject access requests must be made in writing and may be made to any member of the organisation (this includes digital formats).
- All staff who are responsible for responding to subject access requests will follow the processes outlined in detail in GLAS Ltd Subject Access Request Procedures
- Adequate security and storage measures must be in place for the purpose of controlled access, storage, retrieval, the application of subject rights and comprehensive destruction in line with retention schedules.
- If data is found to be incorrect, all copies of the data must be rectified including those copies which have been shared with other persons or organisations as described in the privacy notice and information asset register
- Each data subject must have a chronological record of their shared data kept in their individual file in order to apply the rights of rectification and deletion.
- Personal and special category data must be stored separately to academic files.
- When the risk to a data subject is considered to be high or data is considered sensitive a Data Protection Impact Assessment must be carried out.
- retention schedules for the destruction of data held and to cease processing on that date, except where an extension is deemed appropriate.
- All data breaches of personal or special category data must be reported to the ICO within the 72 hrs
- All data subjects must be informed immediately of a data breach concerning their data.
- All data processed by the organisation as a 'Processor' must be subject to a contract issued by the controller.

Lawful Bases

Consent	the individual has given clear consent for you to process their personal data for a specific purpose.
Contract	the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Legal Obligation	the processing is necessary for you to comply with the law (not including contractual obligations).
Vital Interests	the processing is necessary to protect someone's life.
Public Task	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate interests	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Subject rights

The right to be informed;	The individual's right to be informed under Article 13 and 14 requires you to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice
The right of access;	The individual right of access to data applies in most cases. The data subject has the right to make a subject access request to anyone who holds and processes data about them
The right to rectification;	Under article 16 of the GDPR, if data held on an individual is found to be incorrect or incomplete the organisation responsible for the data must ensure that the data is rectified including all other copies of the data which may have been shared with other persons or organisations. This right is closely linked to the *controller's* obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).
The right to erasure;	Under article 17 of the GDPR, in some cases, individuals have the right to have all relevant personal data erased. This is sometimes known as the right to be forgotten.
The right to restrict processing;	Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances
The right to data	The right to data portability allows individuals to obtain and

portability;	reuse their personal data for their own purposes across different services. Relevant provision = articles 13,20 and recital 68
The right to object	Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.
The right not to be subject to automated decision-making including profiling.	Individuals have the right **not to be subject to a decision when:** • it is based on automated processing; and • it produces an adverse legal effect or a significantly affects the individual.

Exemptions to subject rights in relation to lawful bases

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies.

The remaining rights are not always absolute, and there are other rights which may be affected in other ways. For example, your lawful basis may affect how provisions relating to automated decisions and profiling apply, and if you are relying on legitimate interests you need more detail in your privacy notice to comply with the right to be informed.

Retention schedules

Retention schedules must be set for all categories of data in the context of the data subjects engagement. This will be different for different categories of data and must be included in any privacy statement that may need to be issued because of the processing activity.
Schedules are set by the data controller and not the processor and should be included in any processor-controller contracts or information sharing agreements.

Data Protection Impact assessment

Data Protection Impact assessments must be carried out if when identifying and justifying our lawful basis for processing we also identify a significant privacy impact.

Types of data Covered by GDPR

Personal data

- The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier.
- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
- Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special category data

- The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).
- The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

The following categories are included as special category data: -
Special category data is more sensitive, and so needs more protection. For example, information about an individual's: -

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation.

Glossary:

GDPR	General Data Protection Regulation.
Data Subject	The person or organisation about which the data is held and processed.
Data protection Officer	A person in an organisation responsible for the processing of data and compliance with regulations
Subject access request	When a data subject asks for access to the data which is held and processed about them.
Data protection Impact assessment (DPIA)	An assessment of the potential impact of a privacy breach.
Privacy impact assessment	
Data breach	When data is exposed in a way which is not compliant with the GDPR
Privacy notice	A notice given to data subject regarding the detailed justification and processes involved in the data which will be held and used for a specific purpose.
Lawful basis	The basis on which the data will be held and process.
Retention period	The amount of time that the data will be held.
Data controller	The person or organisation who defines and requires the data to be processed
Data processer	The person or organisation who processes the information on behalf of the Data Controller.
Processing	Obtaining, recording, holding, carrying out an operation on data or information
Information asset	data
Data mapping	Identification of data flows to and from the organisation
Information sharing agreement	An agreement between organisations or persons which outline the procedures for sharing and using information about data subjects.
Personal information	

Date Reviewed:	15/05/2018	Reviewed by:	Steven Jacob
Next Review Date:	14/05/2018	Signature:	

Authorised By:	Position:	Date:	Signature:
Chris Lodder	Director	?	