GDPR & Data Protection Policy

LLSE

Effective from: October 2024

Next Review: October 2025

Version Control		
Date	Owner	Details of Change
October 2023	Andy Fuller	Draft policy sent to DPO (Invicta Law Ltd) for review
November 2023	Andy Fuller	Update following GDPR review – Approved by Board
October 2024	Andy Fuller	Reviewed and approved by Board

Contents

Introduction

LLSE is committed to protecting the rights and freedom of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for delivery and completion of National Professional Qualification (NPQ) and other Leadership Development training programmes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Legislation

The scope of this document sets out compliant practice in line with Data Protection Act 2018 which supports the UK General Data Protection Regulation (UK GDPR) which in turn, is strongly based on the EU GDPR, May 2018.

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Further information can be found via the Information Commissioners Office https://ico.org.uk/

Definitions

Business Purposes	The purposes for which personal data may be used by LLSE: Personnel, administrative, and business development purposes. Business purposes include the following: • Maintenance of business contractual obligations • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as, recruitment, training and quality control, ensuring the confidentiality of commercially sensitive information • Performance management analysis for commissioned contracts • Investigating complaints • Marketing LLSE's business • Improving services

Personal Data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an incident, description or 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 natural person. Personal data we gather may include: • Teacher Reference Number (TRN) • Full name • Previous name (if any) • Gender • Date of birth • Phone numbers • Job role • Ethnic background • Disability (Y/N) • Email address • Working patterns • School (Workplace) Free School meals data • School (Workplace) Ofsted result • School (Workplace) URN • School (Workplace) Name • School (Workplace) Address • School (Workplace) Postcode
Special categories of personal data	The special categories of personal data are • Personal data revealing racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic & biometric data processed for the purpose of uniquely identifying a natural person • Data concerning health • Data concerning a natural person's sex life or sexual orientation
Data Controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, owns the data and determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law. For the purposes of this policy LLSE is the data controller.
Data Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of, and under the instruction of, the data controller.

Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory Authority	This is the national body responsible for data protection, the Information Commissioner's Office.
Data Protection Officer	'DPO' – The primary role of the Data Protection Officer is to ensure that his/her organisational processes, the personal data of its staff, customers, providers or any other individuals (data subjects) in compliance with relevant data protection rules. The DPO for LLSE has been outsourced to a third party, iSYSTEMS Integration Ltd, with named DPO.
Data Protection Lead	'DPL' – is responsible for assisting in monitoring the compliance, training staff, and verifies adherence to the policy on a day to day basis, liaising with the DPO and seeking permissions, advice and guidance as necessary.
Information Commissioners Office	'ICO' upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. LLSE is registered with the ICO for these purposes.

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms, conditions and associated operating procedures. Induction and training will be given to ensure familiarisation.

This policy supplements our other policies where data protection applies. We may supplement or amend this policy with additional policies and guidelines from time to time and as new legislation dictates.

Responsibility for this Policy

LLSE has overall responsibility for day-to-day implementation of this policy which has been reviewed by LLSE's third party DPO service at Invicta Law Ltd. For further information about this policy contact the DPL at enquiries@llse.org.uk.

The Seven Principles of GDPR are:

1. Lawfulness, fairness and transparency - Data collection must be fair, for a legal purpose and LLSE must be open and transparent as to how the data will be used.
2. Purpose limitation – LLSE must be clear about the purposes for processing are
3. Data minimisation - Any data collected must be deemed to be necessary and not excessive for its purpose.
4. Accuracy - The data held must be accurate and kept up to date.
5. Storage limitation - LLSE will not store data longer than is necessary for any contract compliance purposes.

6. Integrity and confidentiality (security) - The data we hold must be kept safe and secure.
7. Accountability - LLSE must ensure accountability and transparency in all our use of personal data.

Our procedures

Fair and lawful processing

LLSE will process personal data fairly and lawfully in accordance with the individual's rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. processing data

LLSE is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

Where LLSE acts as a data processor, we must comply with our contractual obligations and act only on the documented instructions of a data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller.

As a data controller, we must ensure personal data are:

- processed lawfully, fairly and transparently
- processed for specific purposes
- limited to what is necessary
- kept accurate and up to date
- stored for no longer than necessary and
- protected against unauthorised or unlawful processing and accidental loss, destruction or damage

We must also comply with the principles of data protection legislation

As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If anyone is in any doubt about how LLSE handles data, they should contact the DPL initially for clarification who will refer to the DPO if necessary.

Lawful basis for processing data

LLSE must establish a lawful basis for processing data by ensuring that any data we are responsible for managing has a written lawful basis approved by the DPO. It is our responsibility to check the lawful basis for any data we are working with and ensure all of our actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

- Consent - LLSE holds recent, clear, explicit, and defined consent for the individual's data to be processed for the purpose of gaining a relevant qualification or participating in a training event.
- Contract - The processing is necessary to fulfil the qualification or participation in a training event.
- Legal obligation - LLSE has a legal obligation to process the data (excluding a contract).
- Vital interests - Processing the data is necessary to protect a person's life or in a medical situation.
- Public function - Processing is necessary to carry out a public function, a task of public interest, or the function has a clear basis in law.
- Legitimate interest - Processing is necessary for LLSE's legitimate interests or those of a third party. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

In order to process special category data, LLSE must establish one of the six lawful bases listed above and amust also satisfy one of the additional processing conditions set out in Article 9(2) of the UK GDPR.

Deciding which condition to rely on

In making an assessment of the lawful basis, LLSE will establish the necessity of processing such that it is determined to be both targeted and appropriate.

LLSE will consider the following factors and document the answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are LLSE in a position of power over the individual?
- Is the individual a vulnerable person?
- Would the person be likely to object to the processing?
- Are LLSE able to stop the processing at any time on request?

LLSE's commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and to fully justify these decisions.

We will also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Special categories of personal data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories are information about an individual's:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic & biometric data processed for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

In all cases we will only process special categories of personal data where that processing is necessary for the purposes we have identified, we are satisfied that that there is no other reasonable and less intrusive way to achieve that purpose and processing is consistent with the regulatory conditions for processing special category data.

Accuracy and relevance

LLSE will ensure that any personal data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

Individuals may ask that LLSE correct inaccurate personal data relating to them by contacting the DPL/DPO at LLSE with details of the inaccuracy. The DPL will ensure that the erroneous data is corrected.

Data security

LLSE will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPL will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations and will refer to the DPO for any clarification.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place, i.e. behind at least one locked door, where unauthorised personnel cannot access it.
- Data stored electronically will be protected by strong passwords.
- Printed data will be cross-shredded when it is no longer needed
- Cloud based storage will be used wherever possible. Data must not be stored locally on desktops, laptops, tablets or smartphones or on USBs or other portable data storage devices.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures

- All servers containing sensitive data must be approved and protected by security software
- All reasonable technical measures must be put in place to keep data secure

Data retention

- LLSE may provide commissioners with full and free of charge access to all data related to a contract at the end of the term of the contract.
- Where the contract is with Department for Education, hard paper documents containing departmental data should be destroyed in accordance with DfE security standards.
- Data will be retained in line with the LLSE Record Management Policy.

Transferring data internationally

There are restrictions on international transfers of personal data. Before transferring data outside of the UK the advice and approval of the third party DPO will be sought.

Responsibilities

LLSE corporate responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised and monitor and mitigate this risk in a risk register
- Ensuring that data is only retained in accordance with LLSE's Records Management Policy
- Ensuring training of staff

LLSE Data Protection Officer responsibilities

- Inform and advise the organisation and its staff about their obligations to comply with the UK GDPR and other protection laws
- Monitor the organisation's compliance with UK GDPR, other data protection laws and the organisation's own data protection policies
- Advice on and monitor Data Protection Impact Assessments (DPIAs)
- Cooperate with the Information Commissioners Office

LLSE staff responsibilities

- Fully understand our data protection obligations
- Check that any data processing activities comply with our policy and are justified
- Do not use data in any unlawful way

- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through incorrect actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Responsibilities of the Data Protection Lead

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by LLSE
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Identifying, monitoring and mitigating all risks associated with protecting data held
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's GDPR & Data Protection Policy
- Liaising with the DPO on any matters that need DPO permissions or clarifications

Accountability and transparency

The LLSE Data Protection policy will be regularly reviewed and updated, with any changes approved by the DPO and reviewed and accepted annually by the LLSE Board of Directors.

LLSE is responsible for complying with UK GDPR and must be able to demonstrate that compliance by putting in place appropriate technical and organisational measures including:-

- Maintaining up to date and relevant documentation on all processing activities
- Implementing appropriate security measures
- Conducting Data Protection Impact Assessments

Rights of individuals

Individuals have rights to their data which LLSE will respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

    - Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language.
    - Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

    - Individuals have a right to copies of their personal data and supplementary information

- If requested, this must be done without delay, and no later than one month from receiving the request. This can be extended to two months with agreement from the DPO.

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing, and in compliance with all relevant laws

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data on request, so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy notices

When to supply a Privacy Notice:

- A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.
- If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

- If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a Privacy Notice:

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the DPL
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

(Data) Subject Access Requests

What is a subject access request?

- An individual has the right to ask an organisation if they are using or storing their personal information and can ask for copies of any information being stored either verbally, or in writing.

How LLSE deal with subject access requests

- We must provide an individual with a copy of the information requested, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects' access to their information in commonly used electronic formats.
- If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. LLSE will obtain approval from the DPO before extending the deadline.
- We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, or the request is repeated, charge a fee. If the request is for a large quantity of data, we can request the individual specify the specific information they are requesting. This can only be done with express permission from the DPO so they can determine the validity and advise accordingly.

- Once a subject access request has been made, LLSE will not change or amend any of the data that has been requested with the exception of redacting information which is considered to breach other data subjects' confidentiality.

Data portability requests

We will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We will provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This will be done free of charge and without delay, and no later than one month after receiving the request. This can be extended to two months for complex or numerous requests, but the individual will be informed of the extension within one month of receiving the request and the DPO will be notified.

The right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where holding the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child under their guardianship
- And where erasing the data does not contravene other laws

How we deal with the right to erasure.

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims
- And where no other laws are contravened

If personal data that needs to be erased has been passed onto other parties or recipients, they will be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.
- Unless, by doing so other laws are breached

We will inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We will offer a way for individuals to object electronically.

The right to restrict automated profiling or decision making

We will only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

Third parties

Using third party controllers and processors

As a data controller and data processor, we must have written contracts in place with any third party data controllers and/or processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we will only appoint processors who can provide sufficient guarantees under UK GDPR and that the rights of data subjects will be respected and protected.
As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under UK GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts with data controllers and/or data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

As a minimum, our contracts will include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract

- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under UK GDPR
- The processor will assist the controller in meeting its UK GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on UK GDPR.

Audits, monitoring and training

Data audits

Regular data audits will help to inform what personal data is held, where it is stored, how & why it is used, who it is shared with and how long it will be retained for.

Data audits will also help manage and mitigate risks and inform the risk register.

Monitoring

The DPL with contracted support and guidance from the third party DPO, has overall responsibility for this policy. LLSE will keep this policy under review and amend or change it as required. Any breaches of this policy must be reported to the DPL.

Training

Employees will receive adequate induction and training on provisions of data protection law specific for their role. Employees must complete all training as requested. If they move role or responsibilities, they shall be responsible for requesting new data protection training relevant to their new role or responsibilities.

Reporting a suspected data breach

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows LLSE to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify our commissioners of any compliance failures that are material either in their own right or as part of a pattern of failures

Any breach of this policy or of data protection laws will be reported to the DPL as soon as a breach becomes apparent. LLSE has a legal obligation to report any data breaches to our commissioners within set timescales, usually 72 hours.

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

The full reporting process and a template for reporting any suspected breaches is included as Appendix A of this policy.

Failure to comply

LLSE takes compliance with this policy very seriously. Failure to comply puts both the employee and LLSE at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under LLSE procedures which may result in dismissal and termination of contract.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPL at enquiries@llse.org.uk

DPO contact details: Invicta Law Ltd at DPO@invicta.law

Appendix A – Reporting a suspected data breach

If you believe a data breach has occurred, this must be reported to the Data Protection Lead (DPL) using the attached pro-forma and sent to enquiries@llse.org.uk

The DPL will liaise with the Data Protection Officer (DPO)

The DPL, with support from the DPO, will co-ordinate any immediate actions, particularly re containing the breach as far as possible

DPO to assess risk and advise on whether the incident meets the thresholds for notifying the ICO and affected data subjects

DPL and rest of the Senior Team, with support of the DPO, to agree preventative actions to prevent similar types of incidents occurring again.

Data Breach Report Form Template

Your name	
Your work email address and work phone number	
When did this incident occur? (If known, please provide date and exact time).	
Please describe what has happened and how.	
Is personal data involved? If so, please detail.	
How many data subjects have been affected?	
What is the data subjects' relationship with the organisation?	
Who first became aware of the breach, how and when?	

Who was notified about the incident e.g. Line Manager, Data Protection Lead, Data Protection Officer etc. When were they notified and how?	

If there has been a delay in reporting the incident please explain the reasons.	
Has the data placed at risk now been recovered? If so, please provide details of how and when it was recovered.	
From your knowledge of what has happened and the context, please assess likelihood and severity of risk to the data subjects' rights and freedoms. This may include risk of physical, financial, emotional or reputational harm. You should also take into account potential loss of confidentiality, as well as any other social or economic disadvantage that may result.	