Data Protection Policy

At Unloc we are committed to protecting the privacy and security of personal data in compliance with the Data Protection Act 2018 & the General Data Protection Regulation Act 2016. This data protection policy outlines Unloc's commitment to safeguarding personal data collected, processed, stored and managed by our organisation.

This policy applies to all personal data processed by Unloc as the data controller, whether obtained from customers, beneficiaries, employees, suppliers or other individuals. It applies to all employees and third-party service providers who handle personal data on behalf of Unloc.

Principles Of Data Protection:
Unloc adheres to the following principles of data protection:

- **Lawfulness, Fairness & Transparency**:
  - Unlow will process data lawfully, fairly and transparently, ensuring individuals are informed about how their data is processed and used.
- **Purpose Limitation**:
  - Unloc will collect and process personal data only for specified, explicit and legitimate purposes.
- **Data Minimisation:**
  - Unloc will only collect and process personal data that is necessary for the intended purpose and ensure it is accurate and up to date.
- **Storage Limitation:**
  - Unloc will retain personal data only for as long as necessary to fulfil the purposes for which it was collected, taking into account legal, regulatory and business requirements.
- **Integrity & Confidentiality:**
  - Unloc will implement appropriate measures to ensure security, integrity and confidentiality of personal data to prevent unauthorised or unlawful processing, accidental loss or destruction of, or damage to personal data.

Data Collection & Processing:
Unloc will ensure that data is collected and processed within the boundaries defined in this policy. This applies to data that is collected physically or digitally. When collecting data, Unloc will seek consent from individuals for specific purposes and ensure that it is freely given, specific, informed and unambiguous. Unloc's consent processes are transparent, providing individuals with clear information about the purposes of data processing, the types of data collected and their rights regarding their personal information, along with the consequences of not giving consent to processing.

Unloc does not use pre-ticked boxes or ambiguous language in our consent requests and ensures implementation of granular consent. Individuals have the right to withdraw their consent at any time.

As part of Unloc's services we will at times need to collect personal data that is defined as special category data as per Article 9 of the GDPR Regulation 2016:

- Data concerning health.
- Data on race or ethnicity.

Data Security:
Personal data is stored in a secure environment with appropriate technical and organisational measures to ensure it is restricted to authorised personnel for the purposes of delivering services or business activities. Unloc implements access controls, encryption measures and regular security assessments are undertaken as per this policy.

Data Retention:
Unloc retains your personal information for as long as necessary to fulfil the purposes outlined in this policy and as per the regulation. Sometimes we may need a longer retention period when it is required or permitted by law. The criteria used to determine an extended retention period includes:

- Legal, contractual or regulatory obligations that require us to retain information for a specified period. For example, all safeguarding records.
- Business needs, such as managing our relationship, resolving disputes, enforcing our agreements and maintaining accurate records.

A full comprehensive copy of our retention periods can be found at Appendix 1.

Data Sharing & Transfers:

- **Third-Party Processing:**
    - Unloc may share personal data with third parties or agencies such as local authorities, funding bodies and other voluntary agencies when necessary for business purposes. As part of our data collection statement we will ask for explicit consent before sharing this data and ensure appropriate safeguards are in place through contractual agreements and due diligence.
- **International Transfers:**
    - Where personal data is transferred outside the European Economic Area (EEA) or other regions with data protection laws, we ensure adequate protections are in place, such as standard contractual clauses, certification mechanisms or addendums.
- **Special Circumstances:**
    - There are circumstances where the Data Protection Act 2018 allows Unloc to disclose data (including special category data) without an individual's consent. These are;
        - When carrying out a legal duty or as authorised by a government body.
        - Protecting vital interests of an individual or other person or if the individual has already made the information public.

- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities purposes - i.e. race, disability or religion.

Compliance, Monitoring & Review:
To ensure adequate due diligence as part of Unloc's commitment to protecting the privacy and security of personal data we will ensure compliance and review in the form of:

- Mandates:
  - Unloc will ensure it has a Data Protection Officer (DPO) with specific responsibility for ensuring compliance with regulation and legal requirements.
  - All employees processing personal information understands they are contractually responsible for following good data protection practice and are trained to do so.
  - All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.
- Internal Audits:
  - Unloc will conduct regular audits and assessments of our data protection practices to ensure compliance with this policy and applicable laws and regulations.
  - Data protection reviews will be undertaken as part of any new major project or organisational change to ensure practices in this policy have been considered and implemented.
- Policy Review:
  - Unloc will review and update this policy annually to reflect changes in business operations, technology and legal requirements or statutes.

Training:
Unloc will provide regular training and awareness programmes to employees on data protection policies, procedures and best practices to ensure compliance and accountability as the data controller.

Data Breach Management:
In the event of a breach of personal data Unloc will follow the below procedure;

- Quickly establish whether a personal data breach has occurred and, if so, promptly take steps to contain and address the breach.
- Identify the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned. The categories and approximate number of personal data records. Unloc will also identify the likelihood of the risk to people's rights and freedoms.
- Unloc will notify those data subjects who have been affected with;
  - The name and contact details of Unloc's DPO where more information can be obtained.

- A description of the likely consequences of the personal data breach; and a description of the measures taken or proposed to deal with the personal data breach.
- Specific and clear advice to individuals on the steps they can take to protect themselves.

- After review, if it has been identified that there is the likelihood of the risk to people's rights and freedoms Unloc will notify the ICO.

This procedure will be followed through within a 72 hour time period of Unloc becoming aware of a data breach.

Your Rights:
Unloc would like to make you fully aware of all your data protection rights. All service users have the right regarding personal information under the Data Protection Act 2018 & GDPR 2016 regarding your personal information. This includes:

- **The right to access** - You have the right to request Unloc for a copy of your personal data. We may charge you a small fee for this service.
- **The right to rectification** - You have the right to request that Unloc corrects any information you believe is inaccurate or out of date. You also have the right to request Unloc to complete information you believe is incomplete.
- **The right to erasure** - You have the right to request that Unloc erases your personal data, under certain conditions.
- **The right to restrict processing** - You have the right to request that Unloc restricts the processing of your personal data, under certain conditions.
- **The right to object to processing** - You have the right to object to Unloc processing your personal data, under certain conditions.
- **The right to data portability** - You have the right to request that Unloc transfers the data that we have collected to another organisation, or directly to you, under certain conditions.

If you as a service user would like to evoke your right as stated above then please contact Unloc's DPO - dpo@unloc.org.uk and we will respond within a month of this request.
Please note that we may need to verify your identity before processing certain requests.

Contact Information:
If you have any questions or requests regarding this Privacy Statement or our practices, please contact Unloc's data protection officer at;

Data Protection Officer
Unloc
Portsmouth Guildhall, Guildhall Square,
Portsmouth
Hampshire

PO1 2AB
02394008180
dpo@unloc.org.uk
www.unloc.org.uk

This document was approved on the 29th April 2024 and is due for review two years from this date.

----END---

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information Unloc Learning Limited will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Unloc Learning Limited follows its data protection policy and complies with the Data Protection Act 2018.

Individual/Service User – The person whose personal information is being held or processed by Unloc Learning Limited for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of Unloc Learning Limited, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self assessment guide will help you to decide if you are exempt from notification:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).

Special Category Data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

Appendix 1: Data Retention Periods

Personal Data Record Category	Retention Period
Finance	
Payroll records	7 years after audit.
Chart of accounts	Permanent
Financial statements	Permanent
General ledger	Permanent
Invoices	7 years
Business expense documents	7 years
Business card receipts	3 years
Petty cash receipts	3 years
Employee Records	
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	As per legal requirement
Applications for jobs and interview notes	1 year
Payrolls/wages	Duration of employment
Bank details	Duration of employment
Accident books, records and reports	3 years
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years
Whistleblowing documentation	6 months
Right to work in the UK	2 years after employment
Statutory sick pay	3 years
Contracts	
Signed	Permanent
Successful tender & grant documents	Permanent
Customer Data	

Personal Data	Kept until the programme has finished/is disbanded or contractual relationship has completed.
Name, email address in marketing databases	Kept until the person unsubscribes/requests to be removed from our records.
Google Drive folders and files	Reviewed annually, any record/file containing PII deleted by the employee after a maximum of 3 years or as soon as no longer needed.