

Data Protection & Retention Policy

We, Primary PPA cover collect and use (i.e. process) personal data in the course of our activities. We are obliged to comply with the law, in particular the Data Protection Act and the EU General Data Protection Regulation (GDPR), when acquiring and processing personal data.

The aim of this policy is to guide our company personnel in order to meet their legal and contractual obligations in relation to personal data and to communicate to our clients and employees how their data is used and stored.

Data collection and processing

Personal data is information relating to an identifiable individual person.

We only collect and process personal data for lawful reasons. In our case, we collect various categories of personal data relating to individuals who are:

- Customers
- Potential customers enquiring with the company
- Suppliers and other third parties with whom we have dealings
- Directors and employees
- Potential employees

- Pupils of customers, in the event the customer would like assessment data

We collect personal data:

- To comply with our legal obligations, for performance of contracts and for other legitimate reasons
- To deal with enquiries from customers and potential customers
- To keep in touch with customers regarding the service we are providing (which is essential for Ofsted under partnership working)
- To perform a specific activity for which the individual has given us consent.

- To provide assessment and progress reports

In the case of customers who buy our products and services and third parties with whom we have contractual arrangements, we need to keep records of sales etc. for tax purposes and for dealing with complaints, queries and after-sales service.

In the case of directors and employees we have statutory obligations.

When providing news and information as well as marketing to customers and other third parties, we need the written consent of the individuals. This is obtained on our enquiry and booking from when customers enquire or become a client. All customers and others who give consent are free to

withdraw that consent at any time and every email or other communication must give the recipient the right to withdraw consent by clicking on an 'unsubscribe' button.

In any special case, we should obtain consent in writing (preferably by email) before proceeding further.

Data collected by our company

The personal data we collect should be adequate, relevant and limited to what is necessary for our purposes. This means we only collect from:

- Customers, their students and potential customers:

Name and address (email and/or physical address) school phone number, non identifiable information from class registers where reporting is required (uploaded by the schools themselves) - First Name and Second Initial only

- Suppliers, and third parties who provide us with goods and services:

Name, address, bank details plus copies of contracts entered into by them with us and relevant correspondence with them.

- Directors and employees

Name, address, contract details, date of birth and related material from our New Employee Form (as required to be kept on file by law) as well as any appraisals and/or correspondence with them and related documents – e.g. references from a third party.

We take appropriate steps to ensure that all personal data is accurate, accessible (subject to password and authority level controls), complete and compliant with our legal duties.

Sensitive Data includes racial or ethnic origin, trade union membership or political affiliation, data concerning health and sexual orientation. Explicit consent from the individual is needed to process this data unless it is necessary for carrying out specific legitimate tasks. But in all cases great care should be taken to see that the data is kept secure.

As a company we avoid collecting sensitive data except when considered appropriate or necessary.

Data security

Personal data relating to customers, leads and staff is stored on our CRM system on a secure server in the EU (Zoho CRM).

Personal data of employees and of third parties with contractual arrangements with the Company is also stored on the CRM.

All pcs and laptops are password protected with acceptable levels of anti-malware controls. We arrange reviews and updates of our security as appropriate.

All of our contracts are E-Contracts via our CRM system therefore are stored on the aforementioned server.

Personal data is always stored electronically and not in hard copy paper form.

The Company operates a 'clean desk policy' and no personal data should be left on desks or accessible on unattended pcs or laptops.

Third party processors

Some personal data we obtain is processed or held by third parties – including:

- Data relating to teachers criminal record checks has to be entered and processed by *Atlantic Data*. (who process all of our DBS checks)

We undertake due diligence to check that these organisations are competent to deal with personal data and comply with the data protection regulations and have copies of their GDPR compliance policies.

Data retention

We only keep and process data that is necessary for legal and contractual reasons for as long as is necessary or required by law. Generally, this means:

- In the case of customers, for 6 full tax years from the date of purchase, and thereafter until the individual withdraws consent to receiving information from us
- Where the data relates to a contract we have with the individual, for the duration of the contract plus 6 years limitation period,
- Where individuals have agreed to receive newsletters etc., until they unsubscribe or withdraw their consent

All of our feedback forms for customers and employees are online and data is collected anonymously and destroyed once the data has been analysed.

A review of this policy and of personal data will be conducted no less often than yearly and data that is no longer relevant will be destroyed.

Anonymised Data

We may retain data indefinitely in a form that does not include the identity of any individuals – e.g. records of sales of different services, or geographical location of customers - once it has been anonymised or pseudonymised.

Destruction & Disposal of Data

Personal data stored in digital or electronic form will be removed when it is no longer required in a manner that makes it irrecoverable, as far as reasonably practicable.

Personal data in hard copy form that is no longer required will be destroyed by shredding at our premises only.

Rights of Individuals and Procedures for dealing with them

Information to be provided to the individual

When obtaining personal data, it is necessary for us to provide:

- Our name and contact details
- The reasons for processing and the legal basis for it
- Who will be receiving the data (if relevant)
- How long we will keep the data
- Information on the individual's right to access, rectify or require deletion of the information we hold and
- The right to lodge a complaint with the ICO
- Contact details of the data protection officer (if relevant)

We do this online via our Privacy Notice and by asking the individual to consent to our processing their data as they go through any procedure on our website

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information:

- the right to be informed about the collection and the use of their personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances
- rights in relation to automated decision making and profiling
- the right to withdraw consent at any time (where relevant)
- the right to complain to the Information Commissioner

You have the right to request access to your personal we hold about you, we may charge a £10 administration fee for this service . To ask for a copy of the information we hold about you, please contact:

Leah Moore

Primary PPA Cover Ltd Unit T2,

Ivanhoe Park Way,

Ivanhoe Office Park,

Ashby-de-la-Zouch LE65

2AB

Our obligations to provide/rectify/erase information when requested:

If an individual requests information on what personal data we hold on them, we should provide that information within 30 days of the request. This is known as a 'subject access request'. We will

usually require the request in writing and we should take steps to verify that the request is coming from the person he/she claims to be.

If requested by an individual to erase their personal data, we should comply with that request without undue delay. However, if we are required for legal reasons to retain the information (e.g. for tax reasons or because litigation is threatened or in progress), we should inform the individual what data we consider it is necessary to retain for legitimate reasons and only erase it when we consider it is safe to do so.

If consent for retaining personal data is withheld, we should erase the data, subject to the legal points in the previous paragraph. No fee will be charged to an individual for providing/rectifying or erasing personal data. However, if anyone makes repeated requests for personal data we may require a £10 fee before providing it.

Data Breaches

Any breach of security is a serious matter and any data breach may need to be reported to the police and the ICO.

If a data breach is detected, our Operations Manager and DPO Leah Moore should immediately be informed. The breach will be assessed to determine if it needs to be reported to the Information Commissioner or logged in our Data Breach Register, and all necessary procedures will be followed.

Training & Review

All personnel having access to personal data will be given a training session on the GDPR and our Data Protection arrangements. It is mandatory for all of our clerical staff to complete an official GDPR training qualification as part of our onboarding process.

This Policy will be subject to regular review, not less frequently than once a year. That review will include all aspects of the policy and how it is working in practice.