GDPR Policy

GDPR POLICY

PAFA (Parenting Assessments for All) Ltd

1. Introduction

This privacy notice tells you about us, PAFA Parenting and what you can expect when we process your personal data.

1. PAFA Parenting for All is a private limited company and is registered in England and Wales under number 09586193 and a Data Protection Fee payer registered with the Information Commissioner's Office under number ZA500270.
2. Our Data Protection Lead is Barbara Liversage, our Managing Director who is responsible for data protection and our related policies, procedures and/or guidelines.
3. Any questions relating to this Policy, complaints or requests can be referred to Barbara Liversage on info@pafaparenting.co.uk.

2. Definitions

Consent	Your consent, which must be freely given and clearly made (e.g., ticking a box to agree to receive newsletters). You can withdraw your consent at any time by contacting us as above
Data Controller	The person or organisation that determines how and why data is processed. PAFA is the controller of all personal data relating to its staff, job applicants, customers, suppliers and business contacts
Data Processor	A person or organisation that processes personal data on behalf of a data controller. We don't use any data processors for customer data, but do have a limited number for staff data
Data Protection Laws	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR)
Data Subject	An identified (or identifiable) living person. This is included here for your reference, though it is not a term we use in this document, we prefer to just say 'you'!
Personal Data	Any information relating to you and that can identify you either directly or indirectly. If you stop and think about it, there's an amazing amount of data about each of us out there including in our use of the internet, our online services and social media as well as the day-to-day things like our tax, health and employment related information
Personal Data Breach	A security breach that leads to the accidental (or unlawful) destruction, loss, alteration, disclosure of, or access to the personal data we're responsible for
Processing	Pretty much everything that you can possibly do with data is processing – including keeping it in a box or an online system. If it can be filed, it's processing!
Special Category Personal Data	You may know this as 'sensitive data' and it refers to information that if used would cause you additional harm or detriment including ethnicity, political opinions, religious beliefs, trade union membership, health, sexual orientation, and biometric (such as fingerprint scanning) or genetic data. We might process some health data, but we don't process anything else in this category
Subject Access Request (SAR)	Your Right to make a request at any time to find out more about the personal data that PAFA holds about you, what we're doing with it, and why. You can do this on any of the contact methods above

3. Our Approach

The Data Protection Act 2018 is by its nature, written in legal jargon; so, some of the terms and principles we describe have been simplified for ease of reading. If you would like to read the full provisions, you can find them here.

1. The data protection principles state that:

a) we must have a specific reason for processing your information and there are a limited number of those reasons. We can only use your data if we have your consent, or if we need to use it to abide by the law (e.g., health and safety), or to fulfil a contract (e.g. or services or in employment), or where there is a public interest or to protect life, or if we've identified that we need it for our business purposes.

b) We can only collect your data for one of the above reasons and not 'add' another reason without your permission.

c) We should only use the data we absolutely need and nothing else.

d) The information should be as accurate and up to date as possible. You can really help us with this by telling us as soon as you can if something changes.

e) We should only keep it for as long as we need it – we do this by applying expiry/deletion dates to the data we process.

f) Your data must be kept safe. you can be confident that we're using appropriate security and protection systems to defend your data.

4. Your Rights

You have a number of data protection rights. These are:

1. The right to be informed about the data we collect and what we do with it (this notice).
2. The right to find out more about the data we have about you, what we do with it and why (Subject Access Request). You can do this by emailing info@pafaparenting.co.uk or through any of the contacts in the first section. We'll let you know within 2 working days that we've got your request and these are usually completed free of charge within 1 calendar month.
3. The right to ask us to correct any information that is wrong or incomplete. We will do this as soon as we are able to and certainly within 1 month of your request, and we'll let you know when we've done it.
4. The right to ask us to delete your data if we don't really need it anymore, or if you withdraw your consent, or if you're not happy with us using it and we have no legitimate reason to carry on doing so, or if it has been processed unlawfully.
5. The right to ask us to stop processing your data. We will abide by your request but we will let you know if this then means we can't meet our contract with you. Once your request has been agreed, we will likely keep your name and contact email so that we do not inadvertently contact you in the future.
6. The right to object to us processing your personal data if we're using it for the benefit of our business (legitimate interests) (see Section 5). In the majority of cases, we will stop processing it straight away.

You also have the right to complain if you think we've not upheld the law regarding your information. We'd like to know if we got something wrong so that we can investigate and make it right but you can also make a formal complaint to the ICO Make a complaint | ICO

Data we process, why and for how long

In this section, we've separated out the different types of information we process for different groups of people – it may look long, but you can just select the category you'd fall into (customer, enquirer, staff etc.) and check that data table out. Any problems or further questions, please feel free to contact Barbara Liversage using the details in Section 1.

7. CUSTOMERS/CLIENTS

Data	Why We Use It	Lawful Basis	Kept For
Local Authority, name, address and other contact details	Purchase goods/services i.e., Parenting Assessment	Legitimate interests Legal	15 years after service end
Resident Families name, address and other contact details – relevant history, including police reports, psychological/cognitive assessment - sensitive data	Risk Assessment	Legitimate interests Legal	15 years after service end Until the young person reaches age 21

8. SUPPLIERS/CONSULTANTS

Data	Why We Use It	Lawful Basis	Kept For
Company name, address and contact, job title/s	Purchase goods/services	Contract (for services)	2 years after service end
Staff names, contact, job title/s	Purchase goods/services	Contract (for services)	1 year after service end
Contract/service agreement	Purchase goods/services	Contract (for services)	6 years after service end
Company history and data (Companies House)	Due diligence	Legitimate interests	Immediate after service agreement signed
Indemnity insurance	Due diligence	Legitimate interests	3 years after service end

9. ENQUIRERS

Data	Why We Use It	Lawful Basis	Kept For
Company/enquirer name, address, contact, job role	To be able to respond to enquiry	Legitimate interests	1 year after enquiry
Nature of enquiry	To ascertain work needed to fulfil request To meet our legal obligations (Subject Access Request)	Legitimate interests Legal	1 year after response sent 6 months after SAR record closed

10. JOB APPLICANTS

Data	Why We Use It	Lawful Basis	Kept For
Name, address, contact number/ email	To contact you to process your application	Consent	10 days after shortlisting if unsuccessful 1 year after employment ends
Qualifications, experience	Shortlisting for interview	Consent	10 days after shortlisting if unsuccessful 1 year after employment ends

Employment history	Shortlisting for interview	Consent	10 days after shortlisting if unsuccessful 1 year after employment ends
Date of birth or age	May be included on CV	Consent	10 days after shortlisting if unsuccessful 6 years after employment ends

11. STAFF

Data	Why We Use It	Lawful Basis	Kept For
Name, address, contact	Staff file administration	Contract (of employment)	6 years after employment end
Emergency contact details	To know who to contact in an emergency	Legitimate interests	Immediate after employment end
Date of birth	Verify tax Staff administration	Legal Legitimate interests	2 years after employment end
Passport/birth cert/ID card	Proof of Right to work	Legal	2 years after employment end
Driving licence (fleet car users/ mileage claimants)	Insurance cover	Legal	Immediate after employment end
National Insurance No	To ensure your pay is correct	Contract (of employment)	2 years after employment end
Tax code	To ensure your pay is correct	Contract (of employment)	3 years after tax year following employment end
Financial/bank details	To ensure your pay goes to you	Contract (of employment)	3 years after tax year following employment end
Statutory repayments (e.g., student loan)	To ensure your pay is correct and loan payments made	Legal	3 years after tax year following employment end
Baseline Personnel Security checks (staff working on MoD contracts)	To meet our contractual requirements	Contract	Immediate on sending to client company
Contracts, variations, offer letters	To enter into an employment contract with you	Contract (of employment)	6 years after employment end
Health records	Manage absences and sickness. Support you in work	Legitimate interests	6 months after employment end
Grievance records	To allow you to let us know when something has become an issue For us to deal with allegations	Legitimate interests	6 months after employment end
Capability and disciplinary records	To support and improve your performance	Legitimate interests	2 years after date of action or warning issued
Timesheets, overtime and other working time related records	To ensure your pay is correct To ensure we meet our legal obligations	Contract Legal	3 years after end of tax year created 2 years after creation

Records relating to children and young people	To arrange and manage work experience placements	Legitimate interests	Until the young person reaches age 21

We don't send client, supplier, enquirer or job applicant data to anyone else, ever -unless you ask us to refer you to another business contact or client.

For staff, we use data processors for payroll (Wainwrights Accountants), HR consultancy (Concentric Consultancy), Pensions (Aviva). Details can be obtained from Manager Barbara Liversage or Responsible Individual Elaine Karema.

5. Keeping data safe

We told you earlier about the security of our system and staff qualifications but we also make sure that:

a) Electronic copies of personal data are protected by passwords and data encryption and backed up onsite or in the cloud. Backups are also encrypted;

b) All hardcopies of personal data are kept in a locked filing cabinet that only the Senior Management team have access to;

c) We securely delete or dispose of personal data when its no longer needed or has reached its expiry date;

d) All data processing companies that we use are checked for compliance with the data protection laws

e) Staff are trained in data protection

f) Staff lock their computers when they leave their desks

g) Passwords are changed regularly and are required to be sufficiently complex. This is tested occasionally.

6. If it goes wrong

Sometimes despite our best efforts, things do go wrong. If the security of your data is breached, it will be reported immediately to Barbara Liversage who will do the following:

1. If the breach is likely to result in a financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage, Barbara Liversage will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

2. If the breach is likely to result in an even higher risk, she'll make sure that you are directly informed of the breach as soon as humanly possible.

3. Managing a data breach requires a structured and well-coordinated approach to minimize damage, protect affected parties, and prevent future breaches. Here's a step-by-step guide to effectively manage a data breach at PAFA Parenting Ltd:

4. **Activate the Incident Response Team**: As soon as a data breach is detected or suspected, activate your incident response team. This team should consist of individuals with expertise in IT, security, legal, communications, and relevant business areas.

5. **Isolate and Contain the Breach**: Immediately isolate affected systems and contain the breach to prevent further unauthorized access. This may involve disconnecting compromised systems from the network, limiting access to affected areas, or implementing temporary security measures.

6. **Assess the Scope and Impact**: Conduct a thorough assessment to understand the extent of the breach, the type of data compromised, and potential vulnerabilities exploited. This step is crucial for devising an effective

response plan.

7. **Notify Relevant Parties**: Comply with legal and regulatory requirements by promptly notifying affected individuals, regulators, and other relevant parties. Transparency is essential in maintaining trust and credibility.

8. **Engage Legal and Compliance Experts**: Involve legal and compliance teams to navigate the legal obligations, reporting requirements, and potential liabilities associated with the breach. They can guide the organization in fulfilling legal responsibilities.

9. **Communicate with Stakeholders**: Craft clear and transparent communications for affected parties, employees, customers, and stakeholders. Provide information about the breach, steps taken to mitigate it, and actions individuals can take to protect themselves.

10. **Enhance Security Measures**: Conduct a thorough security assessment to identify weaknesses and vulnerabilities that allowed the breach. Implement immediate security enhancements and updates to prevent future incidents.

11. **Recover and Restore Operations:** Work towards restoring affected systems, data, and services to resume normal operations. Ensure that all restored systems are thoroughly vetted for security before being brought back online.

12. **Train and Educate Employees**: Educate employees on cybersecurity best practices and the importance of adhering to security protocols. Regular training sessions can help prevent future breaches caused by human error.

13. **Monitor and Learn from the Incident**: Continuously monitor systems and processes to detect any signs of a recurring breach or new vulnerabilities. Conduct a post-incident analysis to identify lessons learned and update incident response plans accordingly.

14. **Engage External Expertise**: Consider involving external cybersecurity experts to conduct an independent review of the incident and provide recommendations for strengthening the organization's security posture.

15. **Review and Update Policies and Procedures**: Regularly review and update your organization's data breach response plan, cybersecurity policies, and incident response procedures based on insights gained from the breach.

16. By following these steps and maintaining a proactive, collaborative, and adaptive approach to data breach management, PAFA Parenting Ltd can effectively minimize the impact of a breach and work towards preventing future incidents.

7. Implementation of Policy

This Policy shall be deemed effective as of 21/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Barbara Liversage

Position: Director

Signature: 18.10.2023

Rev.	Date	Nature of Changes	Approved/Reviewed By
0.1	10/05/18	First draft	BL
1.0	21/05/18	First version	BL
1.1	02/02/19	Updated to reflect staff changes	BL
	21/05/19	Reviewed – no changes needed	BL

1.2	03/06/21	Reviewed and updated to reflect new UK GDPR	BL
1.3	01/10/22	Reviewed and updated to reflect new UK GDPR	BL
1.4	18.10.23	Reviewed and updated to reflect new UK GDPR	BL

Review Date: 18TH October 2023

Date of Next Review: 18th October 2024