DVACT-PAI
Assessments & Interventions

PRIVACY POLICY OF DVACT-PAI

This is the **Privacy Policy** for DVACT-PAI trading as DV-ACT Ltd.

DV-ACT Ltd is an independent organisation providing domestic abuse services to local authorities, family courts and parents in private law court proceedings. As part of our work, we collect and process personal data about the people who interact with us in accordance with the Data Protection Act 2018 (DPA), The Data Protection, Privacy and Electronics Communications Regulation 2020 (UK GDPR) and any other relevant data protection laws. The kind of data we collect depends on which service is being delivered.

We are committed to protecting your data and privacy, and take great care to ensure it stays safe. This privacy policy will explain how our organization uses the personal data we collect from you and from any referrers. This policy is reviewed annually and updated where required with this version published on 9th June 2026.

This policy includes:

1. WHO WE ARE AND IMPORTANT INFORMATION

2. DATA COLLECTION

3. DATA DISPOSAL

4. RETENTION SCHEDULE

5. WEBSITES AND ONLINE DATA

6. QUERIES, REQUESTS OR CONCERNS

1. WHO WE ARE AND IMPORTANT INFORMATION

What is the purpose of this policy?

Our business will ensure that personal data that we hold is kept secure and that it is held for no longer than is necessary for the purposes for which it is being processed. In addition, we will retain the minimum amount of information to fulfil our statutory obligations and the provision of goods or/and services - as required by the data protection legislation, including the UK General Data Protection Regulation (UK GDPR).

While we've tried to make our privacy policy as comprehensive as possible, it does not include an exhaustive list of every aspect of how we collect and use your personal information. If you need any further information or explanation please contact us using the details below.

Data controller(s)

DVACT-PAI is the trading name for DV-ACT Ltd who is the controller and is responsible for your personal data (collectively referred to as "COMPANY", "we", "us" or "our" in this privacy notice). Our contact details are:

DV-ACT Ltd
71 - 75 Shelton Street
London WC2 H9JQ
Tel: 020 3967 8368
Mob: 07378 423587
Email: Info@dvact.org and programmes@dvact.org
For all data matters contact the data protection officer Claire Verney at info@dvact.org.

Many of our services are provided under sub-contract to experts and we only enter into these arrangements with agencies or individuals who meet our standards around data protection. Nonetheless, whilst your data is in use or being handled by us and being processed or amended by us, we will follow our own protocols as set out here.

2. DATA COLLECTION

Why we collect data

We collect and process personal data about the people who interact with us. The kind of data we collect depends on someone's needs, and how they are using our services. For instance, we might collect data to communicate with someone and send requested information to them, to help us deliver a service that we have been instructed to provide, or to improve our services.

Some of the reasons we might collect your data include:

a) to provide you with the service you have requested or been referred to

b) to record personal details shared during conversations with our assessors and facilitators to ensure we provide the best possible service
c) to record and contact you regarding payments required for self-funded services
d) to process job applications
e) to conduct surveys, carry out research and gather feedback
f) to obtain information to improve our services and user experiences
g) to address and resolve complaints about DV-ACT or our services
h) to comply with applicable laws and regulations, and requests from statutory agencies.

The type of data we collect

Our Company collects the following data:

- Personal identification information (Name, email address, phone number, etc.)
- Details of your case including social services documents, court documents, health data and police data
- Details of the information you give us when attending an assessment interview or session
- Information from forms that you complete as part of an assessment or programme
- Records of your correspondence and engagement with us.

How we use your data

As outlined above we collect personal and sensitive data about individuals. This includes information about health, religion, sexuality, ethnicity, political and philosophical beliefs, and criminal records. We will only use this data when the law allows us to. Generally, we do not rely on consent as the legal basis for processing your personal data; most commonly, we will use your personal data in the following circumstances:

- **Performance of contract:** this means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into an agreement with us to provide a service.
- **Legitimate Interest:** this means processing data for the interests of our business in conducting and managing our business, to enable us to give you the best possible service/product and the most secure experience.
- **Comply with a legal or regulatory obligation:** this means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

How we collect your data

Most of the data we collect is provided by referrers such as social services, solicitors or the courts. We may also receive data directly from parents who wish to self-refer for a programme or assessment, ex- or current partners of self-referrers, or we may collect contact data when we are asked for information about a service directly. We collect data and process data when you:

- Complete an online form to receive information or advice
- Are referred by social services or a solicitor
- Self-refer to us
- Are an ex or current partner of a self-referrer
- Complete a customer survey or provide feedback
- Use or view our website via your browser's cookies.

Sharing your data

If we are working with other organisations or services to support you or your family, we may have to share information with them. We only do this if we have a good reason to and it is necessary for delivering the agreed service. Sometimes we might have to share information with authorities if we think that you or someone else is at serious risk of abuse or harm. We do not need your consent to do this.

We may need to disclose your personal information to third party individuals or organisations in line with our confidentiality agreements. Other organisations we may share your information with include:

- Local authorities concerning child protection measures or care proceedings
- Legal representatives concerning ongoing family court matters
- Family courts directly in relation to ongoing family court proceedings
- The police, if you disclose something that leads us to believe that you, your ex/partner or children may be at risk of harm.

How we store your data

We will keep all your personal information in a confidential record that is specific to your case. We use an electronic case management system and individual assessors and treatment workers may use hard copies of documents. This means that we can keep the information you provide us, so we are able to see the history and relevant details of

your case(s). This ensures that we provide appropriate and accurate assessment reports as well as suitable programme sessions. We take information security very seriously. We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition we limit access to your personal data so that it is only made available to employees, agents or contractors when they need this to provide a service to you, or for one of the other purposes discussed in this notice. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

3. DATA DISPOSAL

We will ensure that personal data is securely disposed of when it is no longer needed.

The method of disposal should be appropriate to the nature and sensitivity of the documents concerned. This includes:

- Non-Confidential records: place in waste paper bin for disposal
- Confidential records: shred documents personally
- Large confidential records: secure shredding service
- Deletion of Computer Records
- Secure drive storage
- Gmail archiving storage.

4. RETENTION SCHEDULE

The retention policy (with its schedule), is a tool used to assist us in making decisions on whether a particular document should be retained or disposed of. In addition, it takes account of the context within which the personal data is being processed and our business practices. We will regularly monitor and audit compliance with this policy and update it when required.

The table below contains the retention period that we have assigned to each type of record. This will be adhered to wherever possible, although it is recognised that there may be exceptional circumstances which require documents to be kept for either shorter or longer periods.

Type of record	Retention period	Where is it stored?	Reason	Method of deletion
Assessment cases				
Referral forms	1 year from last action	- Secure drive - May be kept securely by assessor until filing then moved to drive	a) Deliver service d), e) & f)	- Electronic deletion - Secure shredding
Client contact details (not on referral form)	1 year from last action	- Secure drive- - May be kept securely by assessor until filing then moved to drive	a) Deliver service d), e) & f)	- Electronic deletion - Secure shredding
Letter of Instruction	1 year from last action	- Secure drive- - May be kept securely by assessor until filing then moved to drive	a) Deliver service d), e) & f)	- Electronic deletion - Secure shredding
Court bundles	1 year from last action	- Secure drive- - May be kept securely by assessor until filing then moved to drive	a)Deliver service	- Electronic deletion - Secure shredding
Automated transcript from interviews	Upon completion of handwritten notes	-Zoom icloud -Secure drive	a) Deliver service	-Electronic deletion
Handwritten assessor notes	1 year from last action	- Hardcopy kept in secure location by assessor	a) Deliver service f) & g)	- Secure shredding
Typed assessor notes	1 year from last action	- Secure drive- - May be kept securely by assessor until filing then moved to drive	a) Deliver service f) & g)	- Electronic deletion
Forms completed by clients (inventories etc..)	1 year from last action	- Secure drive- - May be kept securely by assessor until filing then moved to drive	a) Deliver service f) & g)	- Electronic deletion - Secure shredding
Word and pdf versions of DV-ACT assessment reports	Life of the company kept securely on drive	- Secure drive- - May be kept securely by assessor until filing then moved to drive	g) required for court d), e) & f)	- Electronic deletion - Secure shredding
Hard copies of assessment reports	Upon filing of the report	- Kept in secure location by assessor	g) required for court	- Secure shredding
Emails to assessment clients and customers	Archived by gmail at 5 years old	- Google cloud	a)Deliver service c), d), e) ,f) & g)	- Email archiving

Programme cases				
SW Referral forms for a programme	1 year from last action	- Secure drive - May be kept securely by staff until filing then moved to the drive	a) Deliver service d), e) &f)	- Electronic deletion - Secure shredding
Self-referral forms for DAPPs found suitable	1 month from last action	- Secure drive - May be kept securely by staff until filing then moved to the drive	a) Deliver service c), e) & f)	- Electronic deletion - Secure shredding
Self-referral forms for DAPPs found unsuitable	1 month from last action	- Secure drive - May be kept securely by staff until filing then moved to the drive	a) Deliver service & c)	- Electronic deletion - Secure shredding
Court bundles for programmes and suitable DAPP cases	1 month from last action	- Secure drive - May be kept securely by staff until filing then moved to the drive	A)Deliver service	- Electronic deletion - Secure shredding
Court bundles for DAPP cases found unsuitable	1 month from last action	- Secure drive - May be kept securely by staff until filing then moved to the drive	a) Deliver service	- Electronic deletion
Suitability assessment notes and forms for suitable DAPP cases	1 year from last action	- Secure drive - May be kept securely by staff until filing then moved to the drive	a) Deliver service	- Electronic deletion
Suitability assessment notes and forms for unsuitable DAPP cases	1 year from last action	- Secure drive - May be kept securely by staff until filing then moved onto the drive	a) Deliver service	- Electronic deletion
Handwritten programme session notes	Upon transfer to the drive or upon filing of the final report	- Kept secure by facilitator	a) Deliver service	- Facilitator shredding
Electronic notes of all programme sessions	Upon the filing of the final report	- Secure drive	a) Deliver service	- Electronic archiving
LSS notes for DAPP cases found suitable	Upon the filing of the final report	- Secure drive	a) Deliver service	- Electronic deletion
LSS notes for DAPP cases found unsuitable	Upon providing unsuitable letter	- Secure drive	a) Deliver service	- Electronic deletion
Formal letters regarding all cases to/from clients and customers	5 years from last action	- Secure drive - email	a) Deliver service c), e) & f)	- Electronic archiving - Email archiving
Assessor notes for all programmes	1 year from last action	- Hardcopy kept in secure location by assessors - Electronic copy on secure drive	a) Deliver service, b), f) & g)	- Assessor shredding hard copy - Electronic archiving
Word and pdf versions of DV-ACT	Life of the company on secure drive	- Secure drive	g) to comply with requests from agencies	- Electronic archiving

interim and final assessment reports			d), e) & f)	
Emails regarding and to/from programme clients and customers	Automatically archived by gmail at 5 years old	- Email	a) Deliver service b), c), d), e), f) & g)	- Email archiving
Other client/customer data				
Email enquiries	Automatically archived by gmail at 5 years old	- Email	a) Deliver service	- Email archiving
Mondays data - Client names, date tracking and outcome of referrals	Life of the company	- secure drive	a) Deliver service b), c), D), e), f) & g)	- Secure drive - Electronic archiving
Complaints	5 years from last action	- Email - Secure drive	f) address and respond to complaints d) & e)	- Email archiving - Secure drive
Client/customer data that may be kept by other companies				
Self funders paying one off fee for a suitability assessment or risk assessment	See service's own data policies	- Sum up	c) to receive payment for service	See service's own data policies at https://www.sumup.com/en-gb/consumer/legal/privacy/
Self funders paying for programme sessions	See service's own data policies	- Go Cardless	c) to receive payment for service	See service's own data policies at https://gocardless.com/privacy/
Archived emails and secure drive	See service's own data policies	- Google	a) Deliver service b), c), d), e), f) & g)	See service's own data policies At https://policies.google.com/privacy?hl=en

5. WEBSITES AND ONLINE DATA

Cookies

Our website also uses web beacons or pixels through third-party service providers that allow us to track conversions and activity on our website as well as generating advertisements that appear on Facebook and other search engines, like Google, for you and other potential users. Please see our Cookies Policy for more information.

If you receive an email - whether you open it, do not open it, select a link and/or browse our website - we collect this information to ensure that the information we send to people is received and relevant.

When we are monitoring people's online activity in this way, we are using cookies. We use cookies to tailor your browsing experience and ensure we show you more relevant information. If you do not want cookies, you can set your browser to notify you when you receive one, then choose to decline it. Please see our Cookies Policy for more information.

Safe browsing online

If you are in an abusive or controlling relationship it is important you stay safe online. To cover your tracks fully you should **delete your computer's browsing history** as the internet browser you are using will keep records of all websites and webpages you visit. It is important you do not delete everything as this could raise suspicions in an abusive partner, so instead only delete the relevant websites.

Some internet search engines, like Google, keep a record of the words you have used to look for information online. To delete this information, check the settings for the toolbar/browser you use.

Please note: **Deleting your history and toolbar may vary on different internet browsers**. We advise that if you are worried someone will know you are trying to seek help, use a public computer (e.g. at work or in a library) or a friend's device. We do not advise that you search for help on a device you share with your abusive partner. For further advise please visit Refuge's tech abuse website at **https://refugetechsafety.org**

If you are in immediate danger, please call 999.

6. QUERIES, REQUESTS OR CONCERNS

The UK Data (Use and Access) Act 2025 (DUAA) introduced targeted amendments to the UK GDPR and Data Protection Act 2018. Many of its provisions are designed to offer organisations more flexibility and remove red tape, however it also introduces explicit new mandatory requirements for complaints and SAR's.

Organisations must actively facilitate data protection complaints by enabling a clear complaints process which is outlined below. We provide an online form to help you inform us of any complaints and, by law, we must acknowledge your complaint within 30 days, keep you informed, and respond without undue delay.

You can access our online form here

Your rights

Unless subject to an exemption under the data protection laws, you have the following rights with regards to your data:

- The right to request a copy of the personal data which we hold about you;
- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary to retain such data;
- The right to withdraw your consent to the processing at any time, where consent was the lawful basis for processing your data;
- The right to request that we provide you with your personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), where applicable i.e. where our processing is based on consent or is necessary for the performance of our contract with you or where we process your data by automated means;
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to our processing of personal data, where applicable i.e. where processing is based on our legitimate interests (or in performance of a task in the public interest/exercise of official authority).

Please note that the changes to GDPR in 2025 mean that when handling Data Subject Access Requests (DSARs), we are explicitly required to make "reasonable and proportionate" searches, and are permitted to pause statutory timelines if additional information is required to process the request

No fee required – with some exceptions

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable administration fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We will respond to any complaints and acknowledge legitimate requests for data within 30 days.

We aim to respond to data requests within 30 days, occasionally it may take us longer than a month to fulfil a data request if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Queries and complaints

To exercise all relevant rights, queries or complaints in relation to this policy or any other data protection matter between you and us, please in the first instance contact our data protection officer Claire Verney at claireverney.pai@dvact.org

If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with the Information Commissioners Office on 03031231113 or via email https://ico.org.uk/global/contact-

us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England, UK.