

# The Drive Partnership – Privacy Policy

## June 2026

The Drive Partnership is a partnership between Respect, SafeLives and Social Finance.

Staff, systems and governance supporting the partnership’s work are spread across all three organisations, therefore personal information that we process is held in line with the privacy policies for each organisation respectively, but shared between the organisations.

Any queries regarding how we deal with personal information, or this notice, can be referred to [info@drivepartnership.org.uk](mailto:info@drivepartnership.org.uk)

### Privacy policies for partnership organisations:

- Respect: [www.respect.org.uk/pages/privacy-policy](http://www.respect.org.uk/pages/privacy-policy)
- SafeLives: [www.safelives.org.uk/privacy-policy](http://www.safelives.org.uk/privacy-policy)
- Social Finance: [www.socialfinance.org.uk/privacy](http://www.socialfinance.org.uk/privacy)

### How we respect privacy when we deal with personal information

This Privacy Policy applies to information we – The Drive Partnership – collect about individuals who interact with our organisation. It explains:

- what personal information we process under what circumstance
- our legal bases for processing information
- how we use your data
- when we share your data
- how long we keep your data
- rights you have over your data
- why we use cookies on our website
- implications around modifications to this Notice.

### Personal data that we process

The following table explains the types of data we collect and the legal basis, on which this data is processed.

Purpose	Data (key elements)	Legal Basis	How we store your information
You are making a general enquiry or a complaint	Name, email, message	<b>Consent</b> - you have given your active consent.	Stored in the email inbox to which you submit the request. Emails are deleted after 6 months.
You are making an	Name, email,	<b>Legitimate</b>	Information is passed on to the

A partnership between:

information request to us	message	<p><b>interests</b> - it is necessary for us to read and store your message so that we can respond in the way that you would expect.</p> <p><b>Consent</b> - you have given your active consent.</p>	necessary person to answer questions. Stored in the email inbox to which you submit the request
You are sending us a direct message or private message via social media	Name, message, social media handle	<b>Consent</b> - you have given your active consent	Information is stored in the inbox of the social media account you have contacted. All social media accounts are password protected.
You are completing a feedback form or survey with us	Name, email, job title, employer and demographic data, unless otherwise specified (e.g., 'this survey is anonymous')	<b>Consent</b> - you have given your active consent	Information is stored on the survey platform and in a secure location in our IT filing structure.
You wish to attend, or have attended, a training course or event.	Name, email, job title, employer	<b>Consent</b> - you have given your active consent.	This will be held on a web-based service and is password-protected and accessed by training organisers.
You have signed up to receive news and updates from The Drive Partnership.	Name, job title, email address	<b>Consent</b> - you have given your active consent.	Stored securely in a password-protected online email creation platform.
You have registered to access our resources for professionals.	Name, job title, email address	<b>Consent</b> - you have given your active consent.	Stored securely via password-protected website CMS system.
You have sought support and	Personal details, family details,	<b>Consent</b> - you have given your	Anonymised information is stored in password protected folders



<p>guidance via email as a professional who is working with perpetrators of domestic abuse</p>	<p>lifestyle and social circumstances</p>	<p>active consent.</p>	
<p>You are using our website (See section 6 for further detail)</p>	<p>Website activity collected through cookies</p>	<p><b>Consent</b> - you have given your active consent.</p>	<p>This data is anonymous and is stored by Google.</p>
<p>Data on Perpetrators (Service Users) to intervene and reduce likelihood of harm to victims of domestic abuse and assess the suitability of perpetrators to take part in the Drive Project.</p>	<p>Name, personal and contact details. (e.g. age, or DOB, gender).  Family and employment circumstances,  Sensitive data including criminal record, health, racial or ethnic origin, religious beliefs, sexual orientation or political views.</p>	<p><b>Legitimate interests and substantial public interests.</b>  Processing is necessary to Preventing or detect unlawful Acts, Safeguard children and individuals at risk and Safeguard the economic well-being of certain individuals</p>	<p>The information will be stored on a secure encrypted server in the UK.  Full case information will be held on the Drive Project CMS for <b>no longer than 7 years from case closure</b>. For client records, this period is based on 7 years from when the client was last active. For example, if a victim/survivor profile was originally created on a case that closed 7 years ago but is currently connected to an active case which is less than 6 years old, the client would not be deleted.  <b>Records relating to homicide</b>  Data should be kept indefinitely by law enforcement agencies, meaning they are never fully deleted or destroyed. The extended retention period for the most serious crimes is necessary to account for the possibility of future advancements in forensic science or new information emerging that could help solve any cold case.  <b>Where a perpetrator’s sentence includes an indefinite restraining order (made under the Protection from Harassment Act 1997 (POHA 1997))</b>  Data should be held until the date on which the defendant reaches the age of 85 or in the</p>



			<p>year that the sentence is complete if the completion date of the sentence exceeds the age of 85.</p> <p><b>Files in which the defendant is charged, and the case is subsequently discontinued</b></p> <p>Data retained for five years following the date of discontinuance.</p> <p><b>All Child Sexual Abuse (CSA) cases</b></p> <p>Must have an additional 20 years added to the retention date for whatever outcome is reached</p>
Data collected on Victims and third parties.	<p>Name, personal and contact details. (e.g age or DOB, gender)</p> <p>Family circumstances,</p> <p>Details of abuse which may include details of health, ethnicity, sexuality, religion etc.</p>	<p><b>Legitimate interests and substantial public interests and Vital Interests</b></p> <p>Processing is necessary to Safeguard children and individuals at risk.</p>	<p>The information will be stored on a secure encrypted server in the UK.</p> <p>Full case information will be held on the Drive Project CMS for <b>no longer than 7 years from case closure</b>. For client records, this period is based on 7 years from when the client was last active. For example, if a victim/survivor profile was originally created on a case that closed 7 years ago but is currently connected to an active case which is less than 6 years old, the client would not be deleted.</p> <p><b>Records relating to homicide</b></p> <p>Data should be kept indefinitely by law enforcement agencies, meaning they are never fully deleted or destroyed. The extended retention period for the most serious crimes is necessary to account for the possibility of future advancements in forensic science or new information emerging that could help solve any cold case.</p> <p><b>Where a perpetrator’s sentence includes an indefinite</b></p>



			<p><b>restraining order (made under the Protection from Harassment Act 1997 (POHA 1997))</b></p> <p>Data should be held until the date on which the defendant reaches the age of 85 or in the year that the sentence is complete if the completion date of the sentence exceeds the age of 85.</p> <p><b>Files in which the defendant is charged, and the case is subsequently discontinued</b></p> <p>Data retained for five years following the date of discontinuance.</p> <p><b>All Child Sexual Abuse (CSA) cases</b></p> <p>Must have an additional 20 years added to the retention date for whatever outcome is reached</p>
Research	<p>General locality, gender, family circumstances,</p> <p>Details of abuse which may include details of health, ethnicity, sexuality, religion etc.</p>	<p><b>Research exemption.</b></p> <p>Data used to assess success of project, and influence future safeguarding and harm reduction policies.</p>	<p>Data will be fully or partly anonymized meaning individuals cannot be identified from this research data.</p> <p>Data kept indefinitely.</p>
DAPO	<p>Name, personal and contact details. (e.g. age, or DOB, gender).</p> <p>Family and employment circumstances,</p> <p>Sensitive data including criminal record, health, racial or ethnic origin, religious beliefs, sexual orientation or political views.</p>		<p>Full case information will be held on the DAPO Triage CMS for no longer than 7 years from case closure. For client records, this period is based on 7 years from when the client was last active. For example, if a victim/survivor profile was originally created on a case that closed 7 years ago but is currently connected to an active case which is less than 6 years old, the client would not be deleted.</p> <p><b>Records relating to homicide</b></p>

			<p>Data should be kept indefinitely by law enforcement agencies, meaning they are never fully deleted or destroyed. The extended retention period for the most serious crimes is necessary to account for the possibility of future advancements in forensic science or new information emerging that could help solve any cold case.</p> <p><b>Where a perpetrator’s sentence includes an indefinite restraining order (made under the Protection from Harassment Act 1997 (POHA 1997))</b></p> <p>Data should be held until the date on which the defendant reaches the age of 85 or in the year that the sentence is complete if the completion date of the sentence exceeds the age of 85.</p> <p><b>Files in which the defendant is charged, and the case is subsequently discontinued</b></p> <p>Data retained for five years following the date of discontinuance.</p> <p><b>All Child Sexual Abuse (CSA) cases</b></p> <p>Must have an additional 20 years added to the retention date for whatever outcome is reached</p>
--	--	--	--

## How we use your data

We will only use your data in a manner that is appropriate considering the basis on which that data was collected, as set out in the table at the top of this Notice.

For example, we may use your personal information to:

- reply to enquiries you send to us.
- Book you onto a training session, workshop, or any other event that we advertise through our website or online channels.

- where you have specifically agreed to this, send you marketing communications by email relating to our work which we think may be of interest to you.
- understand what aspects of our work people are interested in supporting. Information is analysed anonymously, and it will not identify you.
- fulfil our administrative requirements (for example, completing Gift Aid returns). We may also use your data for analytical purposes however you will not be identified when data is used for this purpose as the data is anonymous.
- Manage the Drive Project and help reduce the frequency and recurrence of domestic abuse thus protecting vulnerable individuals.
- Use research data to inform future policy decisions aimed at reducing domestic abuse.
- Use our research data to inform future policy decisions to reduce domestic abuse.

## When we share your data

The Drive Partnership is a partnership between Respect, SafeLives and Social Finance, with staff, systems and governance spread across all three organisations. Therefore personal information that we process is held in line with the privacy policies for each organisation respectively, but shared between the organisations.

We may share your personal information with third parties where required by law, where it is necessary to administer a contract or agreement with you, to provide a benefit, or where we have a legitimate interest in doing so.

The Drive Partnership work with Police, Local Authorities, MARAC and DAPP Boards and deliver our Drive Project intervention program through third party not-for profit Service Providers. Data is shared between all of these parties, however, very robust local data sharing agreements are always in place to maintain the confidentiality and security of victim and service user data.

We will only pass your data to third parties in the following circumstances:

- Where a legal basis for processing exists and it is necessary to implement the Drive Project or to protect a victim or other vulnerable person.
- We are using a third party purely for the purposes of processing data on our behalf and we have in place a data processing agreement with that third party that fulfils our legal obligations in relation to the use of third party data processors;
- We are required by law to share your data e.g. required by a court of law or the police;
- Where there is a risk that you or someone else is at risk of immediate and significant harm.

- You have provided your explicit consent for us to pass data to a named third party, if required;

All of our third-party service providers are required to take appropriate security measures to protect your personal data in line with Data Protection legislation. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

All data on the Drive Project is held in the UK. We will only pass data to third parties outside of the UK, EEA where appropriate safeguards are in place as defined by Article 46 of the General Data Protection Regulation if adequate safeguards can be guaranteed.

## How we store your personal information and for how long

Your information is securely stored on our secure email server, IT filing systems and password-protected cloud-based platforms.

Where data is collected on the basis of consent, we will seek renewal of consent at least every three years. We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once data is no longer required we will securely delete it in accordance with applicable laws and regulation.

## Rights you have over your data

Under data protection law, you have rights including:

- **Your right of access** - You have the right to ask us for copies of your personal information. All subject access requests will be dealt with by the Data Protection Officer and any requests received will be passed to them immediately
- **Your right to rectification** - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- **Your right to erasure** - You have the right to ask us to erase your personal information in certain circumstances.
- **Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- **Your right to object to processing** - You have the right to object to the processing of your personal information in certain circumstances.

- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.
- **Your right to Complain** - You have a right to complain if you feel that we have not processed your enquiry satisfactorily. You can use [our online complaint form](#) to do this. Whilst you have a right to complain to the ICO they expect data subjects to first try and resolve the matter with the Controller.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

## Contact details

If you have any questions, would like to activate any of your rights you can contact us via [info@drivepartnership.org.uk](mailto:info@drivepartnership.org.uk)

## How to complain

If you are still unhappy after complaining to us, you can complain directly to the ICO.

The ICO's address:

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>

## Cookies & usage tracking

A cookie is a small file of letters and numbers that is downloaded on to your computer when you visit a website. Cookies are used by many websites and can do a number of things, e.g. remembering your preferences, recording what you have put in your shopping basket, and counting the number of people looking at a website. By continuing to browse our websites, you agree to our use of cookies.

We use the following cookies:

- **Strictly necessary cookies**  
These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website.

- Analytical/performance cookies  
These cookies allow us to recognise and count the number of visitors to our website, and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily. We use Google Analytics for this purpose. Google Analytics generates statistical and other information about website usage by means of cookies, which are stored on users' computers. The information collected by Google Analytics about usage of our website is not personally identifiable. The data is collected anonymously, stored by Google and used by us to create reports about website usage. Google's privacy policy is available at <http://www.google.com/privacypolicy.html>.
- Functionality cookies  
These are used to recognise you when you return to the website and record that you are a user of our website, or whether your web browser has Javascript enabled.

### Disabling cookies

You block cookies by activating the setting on your browser that allows you to refuse the settings of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies), you may not be able to access all or parts of our site.

Web browsers may allow some control of most cookies through the browser settings. You can find out more about cookies, including how to see what cookies have been set and how to manage and delete them at [www.aboutcookies.org](http://www.aboutcookies.org). For information on how to do this on a mobile phone, please refer to the handset instructions.

Our websites may also include links to other websites, not owned, associated or managed The Drive Partnership. While we try our best to link only to reputable websites, we cannot be held responsible for the privacy of information collected by sites not managed by us, nor can we accept responsibility or liability for them. For this reason, you should consult the privacy policy on any external website before you submit any personal information to those websites.

## **Modifications**

We may modify this Privacy Notice from time to time and will publish the most current version on our website. If a modification meaningfully reduces your rights, we'll notify people whose personal data we hold and is affected.

## **Policy review**

This Privacy Notice will initially be reviewed after 12 months; from thereon, every 3 years.

Next review date: 01/06/2029