

Privacy notice

How we use your information

This privacy notice explains how Syncora companies and The Calico Group collect, use, store and share personal information. It also explains your rights under UK data protection law, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant changes introduced by the Data (Use and Access) Act 2025 (DUAA). It applies to information we collect about:

- 1. Visitors to our website(s)**
- 2. People who make a complaint to us**
- 3. People who use our services**
- 4. Your individual rights according to UK GDPR**

1. Visitors to our website

When someone visits calico.org.uk & associated company websites, we collect standard internet log information and details of visitor behaviour patterns. We do this to find out information such as the number of visitors to the various parts of the site. We collect this in a way which does not identify anyone. We do not make any attempt to find out the identities of those visiting. We will not associate any data gathered from this site with any personally identifying information from any source. If we do want to collect personally identifiable information through our website, we will be transparent about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

Use of cookies by Syncora companies & The Calico Group

You can [read more about how we use and apply cookies here.](#)

Search engine

Searches and results are logged anonymously to help us improve our website and search functionality. No user-specific data is collected by either The Calico Group or any third party.

Security and performance

Calico Group uses a third-party service to help maintain the security and performance of the website. To deliver this service it processes the IP addresses of visitors to the website.

The IP address (Internet Protocol address) is a numerical label that computers, tablets, smartphones, and other computing devices, use to identify themselves and communicate with other devices.

People who email us

Any email sent to us, including any attachments, may be monitored and used by us for reasons of security and for monitoring compliance with office policy. Email monitoring or

blocking software may also be used. Please be aware that you have a responsibility to ensure that any email you send to us is within the bounds of the law.

2. People who make a complaint to us

When we receive a complaint from a person, we make up a file containing the details of the complaint. This normally contains the identity of the complainant, and any other individuals involved in the complaint.

We will only use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and publish statistics showing information like the number of complaints we receive, but not in a form which identifies anyone. We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that.

However, it may not be possible to handle a complaint on an anonymous basis.

We will keep personal information contained in complaint files in line with our retention policy. This means that information relating to a complaint will be retained for the duration of the commissioned contract.

3. People who use our services

Syncora offer a wide variety of different services to local communities, young people, families, adults and general members of the public.

The personal information we hold on people who use our services will include their contact details, details on why they are receiving support from us and details of their contact with us. However, we only use this information to provide the service the person has requested and for other closely related purposes. For example, we might use information about people who have requested some of our service materials to find out if they would like further support from us. There may be occasions where we will share data with other organisations involved in supporting people who use our services. We will advise if we intend to share data with a third party, however this may not always be possible and any data sharing with a 3rd party will be in line with ICO guidelines.

We will ask service users how they would like us to stay in touch with them during their treatment. Service users can update this information on their preferred contact methods at any time.

All information held by Syncora companies in this regard is subject to strict data protection principles to ensure the security, consistent management and compliance to Information Commissioner's Office (ICO) standards are maintained at all times due to the confidential nature of the data filed.

Service providers reporting a breach

Public service providers are required to consider reporting serious security breaches to the Information Commissioner's Office (ICO). We provide an online form for this purpose, we use the data collected by the form to record the breach, to make decisions about the action we may take, and as relevant in order to carry out those actions.

We retain personal information only for as long as necessary to carry out these functions, and in line with our retention schedule. This means that logs and breach reports will be retained for one year from receipt and longer where this information leads to regulatory action being taken. Syncora & The Calico Group have measures in place to ensure the security of data collected and only processes personal information in line with our policies and procedures.

Retention of personal information

We will keep personal information only for as long as it is needed for the purpose for which it was collected, including to meet legal, regulatory, contractual, safeguarding, audit and reporting requirements. Retention periods vary depending on the type of information and the service involved. Where information is no longer required, we will securely delete, anonymise or archive it in line with our retention schedule.

4. Your Individual rights according to UK GDPR

Data protection regulations have conferred certain rights on you as the data subject regarding your personal data which we hold. These rights include:

- **Right to be informed** about the collection and use of your personal information. This is called 'privacy information'. We are required by data protection regulations to provide you with information regarding the purposes for processing your personal information, the retention period and who it will be shared with. This Privacy Notice serves that purpose.
- **Right of access** to your personal information (commonly known as a "subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. Please contact syncoragovernance@calico.org.uk if you wish to request access to any of your personal information.
- **Right of rectification** – This enables you to have any incomplete or inaccurate information we hold about you to be corrected. Please contact syncoragovernance@calico.org.uk if you wish to rectify any of your personal information
- **Right to erasure** – (also known as right to be forgotten) this enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Right to object** to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. In some cases, we may be able to continue processing if we can show that we have a compelling reason for doing so. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Right to restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

You may also have the right to data portability, the right to withdraw consent where we rely on consent, and rights relating to automated decision-making and profiling. These

rights do not apply in every circumstance. We will explain the outcome of any request and any exemptions we rely on.

You have the right to complain about any matter relating to our service, including how we use your personal information.

In the first instance, please contact our Governance team at syncoragovernance@calico.org.uk or dataprotection@calico.org.uk. Under the DUAA, you can raise a data protection complaint with us directly if you are unhappy with the way we have handled your personal information or responded to a data protection rights request.

We will acknowledge data protection complaints within 30 days of receipt, make appropriate enquiries without undue delay, keep you informed where further time is needed, and tell you the outcome without undue delay. You do not need to use specific legal wording for us to treat your concern as a data protection complaint.

If your complaint relates to our wider service and is not about data protection, we will direct it to the appropriate complaints process.

If you remain unhappy with how we have handled your personal information or your data protection complaint, you may complain to the UK Information Commissioner's Office (ICO) at <https://ico.org.uk/>.

Our ICO registration numbers are:

Calico Enterprise Ltd	Z1745675
Delphi Medical Limited	Z2735447
Acorn Recovery Projects	Z6764409
The Calico Group	ZB210782
SafeNet Domestic Abuse Services	Z7309623

Legal basis for processing data

We will only process personal information where we have a lawful basis for doing so under Article 6 UK GDPR. Depending on the circumstances, this may include processing that is necessary to provide services or support, meet our legal obligations, perform a public task, protect someone's vital interests, enter into or perform a contract, obtain and rely on consent, or pursue our legitimate interests where those interests are not overridden by the rights and freedoms of the individual.

Where we rely on legitimate interests, we will identify the relevant interest and consider whether our use of the information is fair, proportionate and within the reasonable expectations of the individual. Where DUAA-recognised legitimate interests apply, we will still ensure that the processing is necessary, transparent and appropriately documented.

Where we process special category data, such as health information, information about ethnicity, religion, sexual orientation or other particularly sensitive information, we will also identify a condition under Article 9 UK GDPR and, where required, a condition under the Data Protection Act 2018. These may include:

- When this is necessary to protect the vital interests of the data subject or of another person Article 9(2)(c). Vital interests will cover situations where an individual is at risk of immediate and serious harm.
- Data has already been made public by the data subject Article 9(2)(e).
- Processing of legal claims Article 9(2)(f).

Archiving, research or statistical purposes, where appropriate safeguards are in place.

Reasons of substantial public interest, where a relevant condition in the Data Protection Act 2018 applies.

- Preventive or occupational medicine Article 9(2)(h)
- Public interest in the area of public health Article 9(2)(i).

Data Protection Impact Assessments

We consider data protection issues as part of the design and implementation of our systems, services and processes. We do this in order to identify risks associated with data processing, and to take action to mitigate against these risks.

We carry out Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to individuals' rights and freedoms, and before we introduce new or significantly changed systems, services or processes involving personal information.

- Use new systems to process personal data
- Use new tools to communicate with service users
- Process new types of personal data

Sharing information

You have a right to confidentiality (privacy) when accessing our services. However, this right is not absolute and there may be instances where we share your information without your consent.

We may share relevant and necessary information with other health professionals for direct care purposes. We will only share this information to inform and improve decisions about your health and care, and only to those who are delivering care to you or supporting that care. You can object to this, but this may limit the interventions we are able to offer.

Depending on the support you are getting from us, there may be different people, services and organisations who we may be required to share information with. For example, we need to share prescribing information with other healthcare providers (GPs or pharmacies) to keep you safe.

There may also be instances where the law means we have to share information. We will explain this to you and the reasons why. If you would like more information, please contact your service.

If we're concerned about your or someone else's safety, we may need to share information to keep someone safe. Wherever possible we will talk to you about this before it happens.

You can also tell us who you're happy for your information to be shared with – this might be friends, family, or other services you are engaging with. Please know, you can change this information at any time by speaking to a member of staff.

On occasion, we're asked to share information to help improve services and research. We will take steps to reduce the level of information that is shared (such as anonymising data).

We will always strive to ensure that we treat your information with dignity, respect and privacy.

Where we use suppliers, partner organisations or other processors to support our services, we will ensure that appropriate contractual and security arrangements are in place. If personal information is transferred outside the UK, we will ensure that an appropriate transfer mechanism or safeguard is in place.

For services that offer drug and alcohol treatment and support

We share anonymous information about you to show the impact our services are having. The Office for Health Improvement and Disparities collects this information on a database known as the National Drug Treatment Monitoring System (NDTMS). You can find more information about this via your service, or in this [Office for Health Improvement and Disparities document](#). (PDF)

For services that offer prescribed medication

If we are providing medication as part of your support from our services, we will seek your consent to do this. This means we'll tell you about all the possible consequences. This includes potential risks, benefits and side effects. Our doctors and nurses will have conversations with you that will ensure you have the information you need to make an informed decision about your medication options.

Remember, you can change your consent preferences at any time by speaking to a member of staff.

Care Quality Commission (CQC)

The CQC requires us to identify the data flows that fall under Regulation 5 of the Control of Patient Information Regulations (COPI) 2002 and to comply with the national data opt-out. At this time, we do not share any data for planning or research purposes for which the national data opt-out would apply. We review all the confidential patient information we process on an annual basis to see if this is used for research and planning purposes.

Caldicott Guardian

As Syncora is predominantly made up of services that fall under the Health & Social Care sector, A Caldicott Guardian is essential to ensure the ethical and legal handling of personal data. Here are some key reasons why they are needed:

1. **Protecting Confidentiality:** Caldicott Guardians oversee the protection of patient and service user information, ensuring it is used appropriately and confidentially¹.
2. **Ethical Data Sharing:** They help staff make informed decisions about sharing data, balancing the need for information sharing with the duty to protect confidentiality².
3. **Compliance with Laws and Regulations:** Caldicott Guardians ensure that data handling practices comply with relevant laws and regulations, such as the Data Protection Act and GDPR³.
4. **Supporting Better Care:** By ensuring data is used responsibly, they support the delivery of high-quality care and improve patient outcomes¹.
5. **Guidance and Support:** They provide guidance to staff on complex data protection issues, helping to navigate ethical dilemmas and legal requirements².

Data Protection officer

We have appointed a Data Protection Officer (DPO) to oversee our processing of personal information. You can contact the DPO using the details below. We may update these contact details from time to time, but individuals will always be provided with a clear route for contacting the DPO or the data protection team.

Data Protection Officer, Calico Homes Limited, Centenary Court, Croft Street, Burnley BB11 2ED

Telephone: 0800 169 2407

Changes to this privacy notice

Syncora will review this privacy notice at least annually, and sooner where required because of changes to law, regulatory guidance, services or processing activities. Where we make material changes, we will take appropriate steps to bring those changes to the attention of affected individuals.

How to contact us

If you want to request more information about our privacy policy, you can email us or write to:

The Calico Group,
Centenary Court,
Croft Street,
Burnley,
Lancashire,
BB11 2ED

Please address letters for the attention of Syncora Governance & Assurance.

Alternatively, please contact us at **syncoragovernance@calico.org.uk** or **dataprotection@calico.org.uk**

If you are contacting us about a data protection rights request or complaint, please provide enough information to help us identify you and understand your request. We may need to ask for further information to verify your identity or authority to act on behalf of someone else.