



Support Service Data Protection (GDPR) Policy

Context:

Action on Spiritual Abuse Support Services support people in the UK who have experienced harm in spiritual or religious settings. This includes:

- Survivors and victims of spiritual abuse
- People who have been harmed through religion or a spiritual group, even if they wouldn't say they experienced abuse
- People who are supporting others who have been harmed through religion or a spiritual group
- People who are concerned about an unhealthy or abusive organisation or community

The Support Service collects and records certain types of information about our clients.

We will hold information on:

- Personal details of clients who contact us and access our support services including:
 - Name
 - Address
 - Email address
 - Phone number
 - Any needs that may require adjustments to support sessions
 - Minimal details in relation to the Spiritual Abuse experiences they have shared.
- Details of the support that we have provided to clients including:
 - Dates and times of Support Sessions
 - A summary of support given in the session
 - Any significant information shared within the support session especially where this relates to Safeguarding, Domestic Abuse or ongoing risk in relation to Spiritual Abuse.
 - Wellbeing assessments and plans
 - Any unhelpful or abusive behaviours of clients.
- Feedback or suggestions from clients on service improvement which are shared via email rather than the anonymous feedback form

This information is used to provide the best possible service to clients and to monitor and evaluate our service.

Wherever possible clients will be given information about other services and encouraged to self-refer or contact services directly. On rare occasions information about clients may need to be shared for signposting or referral purposes, for example, where a referral by an organisation is needed to access a service. There should be clear and justifiable reasons for the sharing of any information on behalf of a client. The individual's consent will always be sought before any information is shared, except where there is a significant safeguarding concern which requires a referral without consent. Advice from the Designated Safeguarding Lead will always be sought prior to this. Safeguarding Policy can be found on our website.

The Support Service also holds personal information on Employees and Volunteers and contact details of organisations that commission support sessions.

Legislation:

The Data Protection Act 2018 establishes rights and protection for individuals in relation to what information may be held about them and how it may be used.

CASA Support Services fully endorses and adheres to article 5 of the GDPR which states that personal data should be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The Data Protection Act 2018 gives individuals the right to request a copy of any information held about them, this is known as a 'Subject Access Request'.

How we deliver our commitment to Data Protection:

CASA Support Services applies the Data Protection Act principles in relation to collection, use, retention, disclosure and disposal of information.

Information that includes personal data is stored on secure cloud-based servers (Office 365, Monday.com CRM system). Individual client information will only be accessible to the Support Volunteer, their Supervisor and an allocated administrator.

Computers should be locked when staff are away from their desk and if Office 365/CMS/MTC is used from home, and no other person in that household should have access whilst in use. Users must log out of Office 365/CMS/MTC when they are not actively

using the software. The use of USB or any other external storage drives is strictly prohibited.

Printed material is discouraged and any hand-written notes should be destroyed as soon as the CRM system is updated. Any notes that are kept before updating the CRM system should be kept in a locked filing cabinet or drawer.

All support sessions should be undertaken online in a private space where conversations cannot be overheard.

Information held by CASA Support Services relating to clients should only be discussed with Support Managers within the Support Service for example, in a supervision meeting or wellbeing debrief, to gain advice or opinion from their Supervisor. Only information which is relevant should be shared, and details should be discussed discreetly in a private room and not in front of others.

We will store your name and contact details, records of support sessions, wellbeing assessments and wellbeing plans in our CRM system. This system is fully encrypted, and all users are required to use Multi-Factor Authentication each time they log in.

We will also have records of any email communications you have with us and your referral forms. These are fully encrypted and stored securely in Office 365. We have a no emails on phones policy, and all users are required to use Multi-Factor Authentication each time they log in.

Personal information held by CASA Support Services will not be passed to any other agency without the person's consent unless:

- There is a legal obligation to disclose the information
- There are exceptional circumstances justifying a disclosure.

CASA Support Services shall take reasonable steps to ensure that personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

CASA's primary Data Controller is the Executive Manager Simon Plant.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, CASA Data Controller shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO within 72 hours of becoming aware.

All potential breaches or Data Protection issues will be recorded in the GDPR Database which will be accessible only to the Data Controller and Trustees.

File Retention:

It is vital that information is appropriately managed and stored in line with Data Protection legislation, and that it is securely destroyed at the end of the designated retention period.

File retention principles are:

- To ensure that personal data is kept securely and not placed at risk of being lost or viewed by unauthorised persons
- To avoid unnecessary duplication of personal data and have procedures for safely sharing information electronically when appropriate
- To dispose of sensitive information securely at the end of the file retention period

Retention Principles

Data type	Data Management	Access	Required Retention Period
Emails from clients we are unable to offer support.	These will be deleted within 6 months of confirmation that we are unable to offer support. Numbers of will be recorded anonymously.	<ul style="list-style-type: none"> • Recipients only 	6 months
Emails from Clients containing sensitive personal information such as lived experience	These will be stored in the recipient's Office 365 email account. This account will not be accessible on mobiles, is fully encrypted and protected with 2FA.	<ul style="list-style-type: none"> • Support Service Volunteer • Supervisor • Complaints Investigator if complaint made 	7 years after support concluded
Email attachments or shared documents from client	These will be stored in the recipient's Office 365 email account. This account will not be accessible on mobiles, is fully encrypted and protected with MFA. Copies of these may also be uploaded onto our CRM system where relevant. This is fully encrypted and protected with MFA.	<ul style="list-style-type: none"> • Support Service Volunteer • Supervisor • Complaints Investigator if complaint made 	7 years after support concluded
Hand-written notes of Support Sessions	Hand written notes will be destroyed and disposed of by shredding as soon as this information is uploaded to the CRM system.	<ul style="list-style-type: none"> • Support Service Volunteer 	Only as long as necessary to record on the CMS.

			CMS – 7 Years after support concluded
Client Wellbeing Assessment and Action Plan	Wellbeing Assessments and Action Plans will be stored in the CRM system. Any Wellbeing Assessments or Action Plans that exist outside of the CRM will be deleted as soon as uploaded.	<ul style="list-style-type: none"> • Support Service Volunteer • Supervisor • Complaints Investigator if complaint made 	7 years after support concluded
Support Service Volunteer CRM system records	These will be stored in our CRM system where relevant. This is fully encrypted and protected with MFA.	<ul style="list-style-type: none"> • Support Service Volunteer • Supervisor • Complaints Investigator if complaint made 	7 years after support concluded
Non-anonymised Feedback, compliments or suggestions for improvement	<p>This will be anonymised and stored in SharePoint, which is fully encrypted and protected with MFA.</p> <p>The original email will be stored in the recipient's Office 365 email account. This account will not be accessible on mobiles, is fully encrypted and protected with MFA.</p>	<ul style="list-style-type: none"> • Support Service Volunteer • Supervisor • Complaints Investigator if complaint made 	7 years after support concluded
Employee records including personal data, supervision notes, absence data, any disciplinary information	These should be stored in the Employee HR file on SharePoint.	<ul style="list-style-type: none"> • Employee • Supervisor • Complaints Investigator if complaint made 	6 years after leaving, resigning, retiring.
Volunteer records including personal data, supervision notes, absence data, any disciplinary information	These should be stored only in the Volunteer HR file on SharePoint.	<ul style="list-style-type: none"> • Volunteer • Supervisor • Complaints investigator if complaint made 	6 years after ceasing volunteering,
Complaints	All details pertaining to a complaint will be stored in a password protected file on SharePoint.	<ul style="list-style-type: none"> • Complaints Investigator • Relevant Parties as appropriate 	7 years after Support concludes, Employee Volunteer leaves or after the

	<p>Email communication will be stored in the recipient's Office 365 email account. This account will not be accessible on mobiles, is fully encrypted and protected with MFA.</p> <p>Only relevant information regarding the outcome of the investigation and justification for this will be shared with relevant parties</p>		<p>conclusion of the complaint, whichever is latest.</p>
--	---	--	--

All clients, employees or volunteers have the right to request a copy of their records, and/or to ask that their records are deleted before the end of the seven-year period.

Related Policies:

Privacy Statement

Support Service Volunteer Handbook

Safeguarding People Policy

Complaints Policy

Further advice and Resources:

ICO guidance on records retention and storage [Principle \(e\): Storage limitation | ICO](#)

Further reading on the General Data Protection Regulation 2018 <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

Reviewing:

All policies are subject to an annual review and any additional regular review to reflect, for example, changes in legislation or to the structure of policies of CASA

Next Review due: January 2027