Data Protection Policy

Centre for ADHD & Autism Support

Registered Charity Number 1080795

1. Introduction & Background

CAAS is committed to compliance with all national UK laws in respect of personal data, and to protecting the rights and privacy of individuals whose information the organisation collects in accordance with the General Data Protection Regulation (GDPR) and the UK Laws that implement it (**Data Protection Legislation**).

The purpose of the Data Protection Legislation is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge.

This Data Protection Policy (referred to as this **Policy**) is designed to ensure that CAAS complies fully with Data Protection Legislation and that personal data is fairly, lawfully and transparently processed.

CAAS is registered with the Information Commissioner's Office and Kay D'Cruz, Financial Controller is the 'Data Protection Officer'.

2. Scope

The Data Protection Legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details and health information. For the purposes of this Policy references to personal data shall include sensitive personal data or special categories of personal data unless stated otherwise.

The format in which the information is held is in most instances not relevant. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by the Data Protection Legislation.

The application of this Policy is the responsible of all trustees/directors, staff, sessional workers and volunteers of the organisation. You should familiarise yourself with this Policy, CAAS's Confidentiality Policy and other information policies and comply with their terms when processing personal data on our behalf.

3. Purpose and aims of this Policy

To protect the rights and privacy of individuals who access CAAS services, work for, or support CAAS. To ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

4. Policy Statement

CAAS is registered with the Information Commissioner's Office (the **ICO**) to process certain information about trustees/directors, service users, staff, volunteers, sessional workers, staff in external partner organisations and supporters in order to provide the following:

- Governance of the charity
- Provision of support services
- Fundraising, campaigning and membership services
- Monitoring, evaluation and audit of service provision
- Training

When processing personal data in the context of your work with us, you must comply with the six principles of good practice identified in Article 5 of the GDPR. They say the following:

1) **Lawfulness & Fairness:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
2) **Purpose Limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3) **Data Minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4) **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5) **Storage Limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6) **Security:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful

processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In simple terms, this means we must collect and use personal data fairly, tell people how we will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

Partners and any third parties working with or for the organisation, and who have or may have access to personal data, will be expected to comply with the principles of this Policy. No third party may access personal data held by the organisation without having first entered into a third party agreement which imposes on the third party obligations no less onerous than those to which the organisation is committed and which gives the organisation the right to audit compliance with the agreement.

4.1 Data Collection

There are a number of staff at CAAS with different role functions who collect and process personal data. Many of these staff have different rules relating to what they do with the data. Staff should not contravene any of these rules. If you are unsure, please ask a member of the senior management team (Directors or Financial Controller).

'Data Minimisation' is important to think about prior to the collection of any personal data and we should only collect information that is absolutely necessary.

'Data Controllers' must ensure that they have a lawful basis for processing personal data. Under the GDPR there are 6 lawful bases for processing non-sensitive personal data as follows:

1) consent given
2) necessary as part of a contract
3) to comply with a legal obligation
4) to protect the vital interests of an individual
5) to fulfil a public task
6) as part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

Stricter rules apply to sensitive personal data (or 'special categories' of personal data), such as information about a person's health, ethnic origin or religious beliefs as well as information about criminal offences. We can only collect this information under very limited circumstances – for example, the person has given explicit consent or it is necessary for specific reasons permitted by law.

4.2 How does it affect me?

CAAS could be fined if you use or disclose information about other people without their consent or reliance on other lawful grounds. In order to help keep personal data secure, you should take particular care when using the Internet, e-mail or talking on mobile or landline telephones. You could be committing an offence if you steal or recklessly misuse personal data.

Special care must be taken with sensitive personal data (or 'special categories' of personal data) such as information relating to race, ethnic origins, religious/political beliefs, health data, disabilities, sexual life, genetics, biometrics or trade union membership. Details of criminal offences or alleged offences must also be handled with special care.

Any breach of the Data Protection Legislation or this Policy will be dealt with under CAAS's disciplinary, volunteer or governance policies and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

4.3 Responsibilities under Data Protection Legislation

- CAAS is a 'Data Controller' under the Data Protection Legislation.
- The senior management team (Trustees, Directors and Financial Controller) and all those in managerial or supervisory roles throughout CAAS are responsible for developing and encouraging good information handling practices within the organisation. The Data Protection Officer in particular has direct responsibility for ensuring that the organisation complies with the Data Protection Legislation, as do Line Managers in respect of data processing that takes place within their area of responsibility.
- Compliance with the Data Protection Legislation is the responsibility of all trustees, directors, staff, sessional workers and volunteers of CAAS who process personal data.
- Trustees, directors, staff, sessional workers and volunteers of the organisation are responsible for ensuring that any personal data supplied by them, and that is about them, to CAAS is accurate and up-to-date.

4.4 Individuals' Rights

Individuals have the following rights regarding data processing, and the data that is recorded about them:

- The right to be informed about how we process their personal data
- The right to access their personal data
- To right to rectify their personal data
- To right to have their personal data erased
- The right to restrict processing
- The right to have a copy of their personal data in a portable form
- The right to object to direct to marketing and profiling
- Rights in relation to automated decision making and profiling.

If you receive a request, you should forward it on to the Directors immediately. Where a person requests access to their information, this is called a Data Subject Access Request or 'DSAR':

- CAAS must usually respond within one month.
- The response must be in a permanent form, unless this is not possible or the individual agrees otherwise.
- Unintelligible terms must be explained.
- The data must not be changed between receipt of a subject access request and sending the information to the applicant, except for routine amendment of the data which would happen in any case.

4.5 Consent & Transparency

Personal data should not be obtained, held, used or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so. The organisation understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement preferably in writing, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

4.6 Security of Data

All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party unless

that third party has been specifically authorised by the organisation to receive that information and has entered into a third party agreement.

You must not remove personal data from CAAS's premises either in electronic or paper form unless it is really necessary – for example, in cases where staff have to attend external meetings, etc. In instances where data is taken out of the CAAS premises, such data must be fully encrypted and password protected. If data is in a paper format, the staff member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely.

4.7 Disclosure of Data

CAAS must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

All third party without a data-sharing agreement in place requests to provide data must be supported by appropriate paperwork and specifically authorised by the Data Protection Officer.

4.8 Retention & Disposal of Data

Personal data may not be retained for longer than it is required, eg after a member of staff has left CAAS, it may not be necessary to retain all the information held on them. Some data will need to be kept for longer periods than others. CAAS's retention and data disposal procedures will apply in all cases.

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg shredding, disposal as confidential waste, secure electronic deletion.

Personal data may need to be kept for a certain period of time under other legislation such as accounting, employment or tax laws. In such cases reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

Duplicate copies of personal data should not be kept as doing so increases the risk of that data being compromised. CAAS's secure cloud-based database system should be the central electronic record of personal data for stakeholders. Where there is a need to have two copies of personal data for a short timeframe to complete a task one copy should be deleted as soon as it is no longer needed.

4.9 Working with third party partner organisations

All CAAS projects funded in partnership with other third party organisations should include within the contractual agreement a clear statement as to the extent to which CAAS and the third party partner organisation is responsible for compliance with Data Protection Legislation (as Data Controller and/or Data Processor) and the respective obligations of CAAS and the third party partner organisation with regard to data protection.

In addition, any external parties such as contractors with access to personal data during the course of their work will be required to conform to CAAS confidentiality standards and this Policy and must demonstrate their agreement in writing.

4.10 Personal Data Breaches

A Personal Information Breach is for example, loss of a memory stick or accidental disclosure of personal data to a third party.

You should report all breaches to the Directors who will decide how to respond to the breach and whether it needs to be notified.

4.11 Anonymisation

'Anonymisation' is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymising personal data significantly reduces the risks to individuals if that information is compromised.

Where personal data is collected and needs to be retained for statistical purposes, but it no longer needs to be attributable to an individual it should be anonymised at the earliest opportunity.

Fully anonymised data can be difficult to achieve in some situations. Where this is the case it is still good practice to partially anonymise the data to lower the chance of it identifying an individual.

5. Roles and Responsibilities

5.1 Senior Management

Overall responsibility for compliance with Data Protection Legislation rests with the CAAS Board of Trustees. The Board is responsible for making sure that the Data Protection function is fully resourced to meet the needs of CAAS.

5.2 Quality and Compliance

The senior management team (Directors and Financial Controller) monitor and review the operation of this Policy and receive feedback from line-managers and staff team members. The senior management team reports to the Board of Trustees and ensure operational adherence to the Policy including:

- understanding and communicating obligations under the Data Protection Legislation
- identifying potential problem areas or risks
- producing effective procedures
- notifying and annually renewing notification to the Information Commissioner

5.3 Line-managers

Line-managers are responsible for promoting data protection awareness and compliance with Data Protection Legislation and this Policy their teams, sessional workers and volunteers. Line-managers are also responsible for making sure that all their staff, sessional workers and volunteers have been accorded the necessary data protection training.

5.4 All Trustees, Staff, Sessional Workers and Volunteers

It is the responsibility of all trustees/directors, staff, sessional workers and volunteers to ensure they understand and act in accordance with this Policy and Data Protection Legislation. Staff, should also ensure that they keep the Data Protection Officer updated if they become aware of any proposed changes or changes to the ways in which personal data is being processed by their team.

Trustees, directors, staff, sessional workers and volunteers found to be acting contrary to this Policy may be subject to action under disciplinary, volunteer or governance policies. This is because any breach of the Data Protection Legislation could result in CAAS facing legal action.

Appendix A: Glossary of terms for the General Data Protection Regulation (GDPR)

Accountability – the data controller is responsible for compliance with the data protection regulations. They must also be able to demonstrate the steps the business takes to ensure compliance.

Anonymisation - the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual).

Consent – consent is defined as receiving a data subject's agreement to process their data. Agreement must be freely given, informed, specific and unambiguous. This consent could be given several ways, such as via a written statement (including by electronic means) or an oral statement. Gaining consent must be clear and unambiguous. The data subject must understand implicitly what they are providing their data for, how it will be processed, who will process it and how long it will be stored.

Data Breach – any accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access of a subject's data.

Data Controller – 'controller' means the legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data.

Data Erasure– (also known as the Right to be Forgotten) this entitles the data subject to request that the data controller erase their personal.

Data Minimisation – this means that you can only collect personal data if it's needed to achieve the intended purpose. Personal data should be adequate, relevant and limited to what is necessary. Where appropriate, such data should also be kept up to date.

Data Processor – 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. 'Processing' means any operation, or set of operations, which is performed on personal data or on sets of personal data. It is considered processing whether these operations occur by automated or manual means. Processing includes the following activities: collecting, recording, organising, using, structuring, storing, adapting, retrieving, consulting, destroying and more. The data processor can be an organisation or third-party provider who manages and processes personal data on behalf of the controller. Data processors have specific legal obligations, such as maintaining personal records, and are liable in the event of a data breach.

Data Protection Authority – the national authority who protects data privacy. In the UK, this is the Office of the Information Commissioner.

Data Protection Officer – an appointed individual who works to ensure you implement and comply with the policies and procedures set by GDPR.

Data Subject – someone whose personal data is processed by a controller or processor.

Data Subject Rights – the data subject has the right to:

1) Transparency (to be informed).
2) Access the data.
3) Rectify the data.
4) Request that the data be erased.
5) Restrict processing.
6) Data portability.
7) Object to the processing of data.
8) Not to be subject to a decision based solely on automated processing.

Data Subject Access Request (DSAR) - Under the Data Protection Legislation, individuals have a right to understand how an organisation is processing their personal data and have access to their information. This is called a Data Subject Access Request or 'DSAR'. In exercising this right, an individual can contact us at any point to request copies of the personal data we hold about them, why we are processing it, whether it will be shared with any third parties and request details of the source of the data.

Encrypted Data – personal data which has been translated into another form or code so that only people with specific access can read it.

EU-US and Swiss Privacy Shield – this refers to a framework which allows companies to comply with data protection requirements when data is transferred to, or via, the EU and Switzerland and the USA. If a company has the shield in place it allows for the legal transfer of personal data between the EU and US for commercial reasons.

Integrity & Confidentiality Security – personal data must be processed using appropriate technical, organisational and security measures.

Legal Processing – for any personal data processed, the organisation must be able to specify that it has been processed on one of the legal grounds specified by GDPR. These grounds are:

1) Individuals consent.
2) Contract with the individual (including pre-contract arrangements).
3) Complying with a legal obligation.
4) If it is in the vital interest of the data subject.
5) Necessary for a task in public interest or authority.
6) Necessary in the legitimate interest of an organisation or third party (balanced against interests of the data subject).

Personal Data – any direct or indirect information relating to an identified person that could be used as a means of identifying them. This includes their name, ID number, location data or an online identifier, photograph.

Privacy Impact Assessment – a tool used to identify the privacy risks if a change in how an organisation runs causes a substantive change in how it processes personal data which could present a high risk to individuals.

Profiling – the automated processing of personal data.

Processing – this refers to any activity relating to personal data, from initial collection through to the final destruction. It includes the organising, altering, consulting, using, disclosing, combining and holding of data, either electronically or manually.

Pseudonymisation – the separation of data from direct identifiers so that linkage to an identity is not possible without additional informationthat is held separately.

Purpose Limitation – this refers to using information only for the specified, explicit and legitimate purposes for which the data was collected and not for any other purpose.

Special Category Personal Data – more sensitive information relating to a data subject. Includes information which reveals a person's: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Third Party – a legal body or authority other than the data subject, controller or processor who is authorised to process personal data under authority of the data controller or processor.

Signed: _____ **Position:** _____

Date: _____

Date first issued: January 2017

Reviewed and Amended: June 2018

Next review date: January 2021