Approved Board: 5/2/25

Data Protection Policy

Context

Data protection is the practice of safeguarding personal data by applying data protection principles and complying with applicable data protection law.

This policy provides a framework for ensuring that CAAS meets its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 18).

Introduction

The Centre for ADHD & Autism Support (CAAS) is a charity based in Northwest London. We are here to support ADHD and Autistic individuals, families, and professionals. Our vision is to raise awareness, break down barriers and drive lasting positive change for neurodivergent people in our community. We do this by focusing on our aims, which are to support, educate and empower individuals by providing a range of services and support, including individualised support for young people and adults, courses, social groups, trainings and workshops.

CAAS is committed to protecting the rights and privacy of individuals, and to ensuring that personal data is processed in accordance with data protection law. This Data Protection Policy (referred to as this Policy) is designed to ensure that CAAS complies fully with data protection legislation, that personal data is fairly, lawfully and transparently processed in accordance with the data protection principles outlined below, and that the rights of data subjects are protected.

Scope

Data protection law 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.

Some personal data is more sensitive in nature and is afforded more protection in law, for example information related to race or ethnic origin, religious beliefs, health data or sexual orientation.

CAAS collects both personal and sensitive information, so for the purposes of this policy any references to 'personal data' shall include 'sensitive personal data' or special categories of personal data unless stated otherwise.

CAAS is a 'Controller' under data protection law. Data is processed by CAAS in order for it 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 (internal and external)

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 for example, it is covered by this policy.

This policy applies to all individuals working on behalf of or representing CAAS, including trustees, staff, and volunteers. Any breach of this policy may result in disciplinary action.

Principles

CAAS is registered with the UK Information Commissioner's Office (ICO), which provides guidelines on data protection that CAAS will follow. Any personal data processed by CAAS will be:

1. Processed lawfully, fairly and in a transparent manner.
   - There are several grounds on which data may be collected, including consent.
   - We are clear that our collection of data is legitimate, and we have obtained consent to hold an individual's data, where appropriate.
   - We are open and honest about how and why we collect data and inform individuals about their rights, including their right to access their data.

2. Collected for specified, explicit and legitimate purposes and not used for any other purpose.
   - We are clear on what data we will collect and the purpose for which it will be used.
   - We only collect data that we need.
   - When data is collected for a specific purpose, it may not be used for any other purpose unless allowed by law.

3. Adequate, relevant and limited to what is necessary.
   - We collect all the data we need to fulfil our work.
   - We don't collect data that we don't need.

4. Accurate and, where necessary, kept up to date.
   - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as client, staff or volunteer records.
   - We correct any mistakes promptly.

5. Kept for no longer than is necessary.
   - We understand what data we need to retain, for how long and why.
   - We only hold data only for as long as we need to, including both paper and electronic data.
   - Some data must be kept for specific periods of time (eg financial or staff data).
   - We have an archive policy that ensures data no longer needed is anonymised or destroyed.

6. Processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage.
   - We develop, implement and maintain technical and organisational safeguards appropriate to our size, scope and available resources, the nature and amount of Personal Data that we hold and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.
   - Data is held securely, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected.
   - Data is kept safe. Our IT systems have adequate anti-virus and firewall protection that's up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
   - Data is recoverable. We have adequate data back-up and disaster recovery processes

We are responsible for and must be able to demonstrate compliance with the data protection principles listed.

Other applicable policies and procedures

Our commitment to these principles means that we will ensure we can evidence our compliance with them. We recognise that failure to do so can put individuals at risk and can result in breach of legislation, reputational damage, or financial implications due to fines.

To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on data protection as follows:

- Annual mandatory GDPR training
- Privacy notice
- Confidentiality Policy
- Handbook, containing code of conduct and information on technology usage
- IT Policy
- Safeguarding Policy
- Ethical Fundraising Policy

Data Collection

CAAS collects a variety of information, at different contact points relating to our service users, staff and other individuals.

CAAS collects data, including personal data, relating to service users and other individuals in the course of its activities. CAAS also collects data, including personal data, about staff members through the application, recruitment and on-boarding processes and in the course of job-related activities throughout individuals' engagement with CAAS.

Our privacy notice sets out the legal basis on which this data is collected and stored, and all representatives of CAAS are responsible for ensuring they are compliant.

Staff are expected to take particular care with sensitive personal data, and when using the Internet, e-mail or talking on mobile or landline telephones. Staff know that they could be committing an offence if they steal or recklessly misuse personal data. Any breach of the data protection law or of 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 may require notification as soon as possible to the appropriate authorities.

Most of the data which CAAS collects is stored on our Charity Log CRM system behind password access controls, and is automatically backed up. Data hosting is from EU sites.

Additional data is also stored in our Microsoft 365 IT system, which has restricted file access, is automatically backed up, and has appropriate cyber security in place. Files which contain identifiable personal data are also password protected individually. Data hosting is from EU sites.

Some personal data is held by trusted suppliers, such as Mailchimp (our email system) and Eventbrite and Zoom (our training and event platforms). These suppliers have their own privacy notices which you can view, and are well known providers with appropriate data protection procedures.

Minimal paper copies of data are retained, and any paper registers or similar that are taken are shredded as soon as they have been entered into the relevant CAAS IT system.

Special Category Personal Data / Criminal Convictions Data

We take the security of special (or sensitive) categories of personal data, children's data, and criminal convictions data very seriously. We have safeguards in place to protect personal data against unlawful or

unauthorised processing, or accidental loss or damage. We will ensure that where special categories of personal data, children's data, or criminal convictions data are processed, that:

- Where we no longer require special categories of personal data or criminal convictions data for the purpose for which it was collected, we will securely delete it or render it anonymous as soon as possible.
- Where records are destroyed we will ensure that they are safely and permanently disposed of.

We ensure that we process special categories of personal data, children's data or criminal convictions data under an appropriate lawful processing condition.

Consent

Sometimes our lawful basis for processing personal data may be consent. Where a data subject agrees to us processing their personal data, they must clearly indicate consent through a positive, opt-in action. If an individual gives consent in a document which also deals with other matters, then the consent must be separate from those other matters.

Data subjects must understand that they can easily withdraw their consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed where we intend to process personal data for a different incompatible purpose which was not disclosed when the data subject first consented.

Where consent is required, CAAS must be able to evidence how the consent was captured and keep records so that CAAS can demonstrate compliance with consent requirements.

Specific Roles and Responsibilities

Complying with this policy is the responsibility of all staff and any other individuals who work for or represent CAAS. In particular, they should promptly raise any concerns around data protection with their line manager and with the Data Protection Lead.

Specific responsibilities under this policy are also noted as follows:

- Board. Overall responsibility for compliance with data protection law 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.

- Senior Leadership Team. The senior leadership team monitor and review the operation of this policy and receive feedback from line-managers and staff. They report to the Board of Trustees and ensure operational adherence to the policy. In particular this responsibility includes producing effective procedures, identifying and addressing potential challenges and communicating obligations around data protection across the organisation. They are also responsible for advising on and assessing compliance with the policy, and with UK legislation, and on making recommendations to improve compliance.

- Finance & Admin Team. The finance team are responsible for ensuring annual renewal of membership of the ICO, and for retaining training records demonstrating staff compliance with their annual mandatory GDPR training.

- Line-managers are responsible for promoting data protection awareness and compliance with this policy within their teams, and for undertaking performance management with anyone who is not in compliance, or who needs additional support to fully comply.

- Data Protection Lead (DPL). CAAS will appoint a Data Protection Lead who will be responsible for overseeing data protection, and leading on any incident investigation and reporting. The Data

Protection Lead will also ensure that all staff, sessional workers and volunteers are provided with induction and on the job training, and made aware of their data protection responsibilities.

The CAAS DPL is Rebecca Murphy, and she can be contacted on rebecca@adhdandautism.org

Individual Rights and Data Retention

We recognise that individuals' rights include the right to be informed, of access, to rectification, erasure, restrict processing, data portability and to object and withdraw consent. Our privacy notice sets these rights out in more detail.

Our privacy notice also sets out our approach to managing data when we work with children or other more vulnerable people.

The amount of time we retain information for varies depending on the type of information stored. We only retain personal data for as long as necessary to fulfil the purposes it is collected for. Factors affecting retention periods include legal requirements, storage costs, historical value, industry standards, and archival needs. Some examples of the retention periods for the data we hold at CAAS can be found in the Privacy Notice. Our privacy notice outlines our approach to data retention.

Personal data will be securely disposed of in a way that protects the rights and privacy of data subjects (eg shredding, disposal as confidential waste, or secure electronic deletion) and in accordance with our legal obligations and our relevant policies and procedures.

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

Working with Others

All CAAS projects funded or delivered in partnership with other third-party organisations will 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 law (as Controller and/or 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.

Data Subject Rights Requests

Any Data Subject Rights Requests (DSRRs) received should be forwarded to the DPL immediately, and on receipt CAAS commits to ensuring:

- Steps are taken to verify the identity of the individual making the request.
- A response within one month (unless an extension of a further two months is deemed appropriate).
- Unless otherwise requested by the requester, the response will be provided in a commonly used electronic form.
- The relevant data will not be changed between receipt of a request, and CAAS sending the information to the requester, except for routine amendment of the data which would happen in any case.
- Full and accurate records will be maintained.

Fundraising and Marketing

We will ensure that our fundraising complies with the Data Protection Act, ICO guidelines and the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors and other individuals and will respond promptly to requests

to cease contacts or complaints and act to address their causes.

Whenever we rely on a data subject's prior provided consent, it will be made clear that consent can be withdrawn. Data subjects will be clearly and explicitly informed of their right to object to direct marketing, and this will be distinguishable from other information. For example, in emails, this may take the form of a simple 'unsubscribe' link in email footers.

If a data subject opts-out of direct marketing, this request will be promptly honoured, and their contact details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future (e.g. a do-not-contact email list).

Automated Decision-Making (ADM)

ADM occurs where a decision affecting an individual is made entirely by automated means. Examples of ADM may include an automated credit scoring system or a computerised candidate c.v. or psychometric evaluation system. CAAS does not currently carry out any ADM activities.

Data Breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Any staff or other individual who becomes aware of a personal data breach (or suspects one) related to personal data that CAAS holds or processes must notify the DPL immediately.

We will investigate the circumstances of any data breach or suspected data breach, to identify if any action needs to be taken. In the event of a breach, we will carry out an initial assessment to determine:

- what is the nature of the incident (loss, theft, network security issue etc)?
- what data / systems are affected?
- who / what has caused the breach?
- is the cause / risk / threat ongoing?
- are any other systems, networks, data storage facilities at risk?
- are any individuals affected by the breach (e.g. service users, staff, other data subjects etc.)?
- if so, what are the risks to the rights and freedoms of those individuals and are the risks high?

We will also take immediately available steps to contain, secure and resolve the data breach.

Remedial action might include changes in procedures, where these will help to prevent reoccurrence, or disciplinary or other action, in the event of negligence.

We will notify the ICO within 72 hours after becoming aware of a personal data breach if it is likely to result in a risk to the rights and freedoms of individuals or if it is likely to have a significant detrimental effect on individuals. For example, we will notify the ICO if a breach might result in discrimination, damage to reputation, financial loss or significant social disadvantage. In any case, we will keep a record of any personal data breach (including our decision relating to whether to notify the ICO).

Equality, Diversity and Inclusion

CAAS is committed to providing services which embrace diversity and that promote equity in opportunity. Everyone who accesses our services or who represents us in a paid or voluntary capacity should be safe, empowered to play a part in promoting their own welfare and that of others, and be able to live a life free from abuse. This applies to all, regardless of age, sex, ethnicity, disability, sexuality or belief, however we recognise that some children and adults at risk from harm may be additionally vulnerable, because of the impact of discrimination, previous experiences, their level of care or support needs, or other circumstances. We will ensure that our approach to data protection and privacy understands the implications of such inequalities, and pay particular attention to supporting those less able to protect their own data and keep it safe.

Training and Audit

We ensure all staff have undergone adequate training to enable them to comply with this policy and will also regularly test our systems and processes to assess compliance. Staff must attend all mandatory data protection training.

Staff must regularly review all systems and processes under their control to ensure they still comply with this policy and check that adequate controls and resources are in place to ensure proper use and protection of personal data.

Ownership, Review and Monitoring

This policy is owned and approved by the Board.

It will be reviewed every two years, or sooner if needed, should legislation or best practice change. The CEO and DPL will also review this policy, and the processes and procedures which surround it, in the event of a substantive data breach, to ensure any learnings can be incorporated within our practice, or the policy improved where appropriate.

Appendix One : Glossary

UK GDPR: The retained EU law version of the General Data Protection Regulation ((EU) 2016/679).

Processor: An individual or organisation that processes personal data on behalf of a controller.

Controller: An individual or organisation that determines how and why personal data is processed. The Controller is responsible for compliance with the DPA and GDPR

Data Subject: An identified or identifiable living individual whose personal data is being processed.

Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.

Personal Data: Any information that can identify a data subject, such as name, address, or email address. This includes not just being identified by name but also by any other identifier such as ID number, location data or online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

Sensitive or Special Category Personal Data: Personal data revealing 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 an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.

PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.

Valid Consent: Agreement, which is freely given, specific, and informed, and is an unambiguous indication that a data subject agrees to the processing of personal data relating to them.

Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the controller or a third party.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

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). 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.

Criminal Convictions Data: Personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.