HACS
Hillingdon Autistic Care & Support
Registered Charity Number 1066859

DATA PROTECTION POLICY AND PROCEDURE

Rationale

Our data protection policy sets the Charity's commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data. HACS is committed to ensuring that we comply with the law regarding Data Protection and that data subjects (the people that we hold data on) are satisfied with how their data is collected and used.

The policy covers all aspects of the Charity's work relating to personal information and includes all methods of holding and storing information, including:

- Manually stored paper data
- Data stored on computer hard drives and backed up on a secured server
- Computer referenced paper data (e.g. databases)
- Data held in computer applications
- Data held in records archive storage
- Data held on portable storage devices

Legal Context

This policy aims to ensure the charity collects, stores and processes data in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which determines how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data. The regulation applies to all organisations that store and use personal data, and will apply even after the UK leaves the EU. The main principles

of the GDPR sets out the key principles that all personal data must be processed in line with. Data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

There are also stronger rights for individuals regarding their own data. The individual's rights include:

- to be informed about how their data is used
- to have access to their data
- to rectify incorrect information
- to have their data erased
- to restrict how their data is used, to move their data from one organisation to another
- to object to their data being used at all

Definitions

'Personal data' means information that can identify a living individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

'Special category data' is personal data which the GDPR considers more sensitive, and so needs more protection. In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. This includes, but is not limited to information about an individual's race, ethnic origin, religion, trade union membership, sexual orientation, genetics or health.

'Processing' refers to anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

'Data subject' is the identified or identifiable individual whose personal data is held or processed.

'Data Controller' is a person or organisation that determines the purposes and the means of processing of personal data.

'Data Processor' is a person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

'Personal data breach' constitutes a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Data Controller

The Charity processes personal data relating to service users, staff, Trustees, visitors and others, and therefore is a data controller. HACS is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

Roles and responsibilities

This policy applies to all staff employed by the Charity, Trustees and volunteers. The policy also extends to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The Trustees have overall responsibility for ensuring that the Charity complies with all relevant data protection obligations.

The GDPR requires organisations to appoint a Data Protection Officer (DPO). The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPO will report to the board their advice and recommendations on data protection issues. The DPO is also the first point of contact for individuals whose data the Charity processes, and for the ICO.

Our DPO is *Stephanie Mullally* and is contactable via *stephanie@hacs.org.uk.*

All staff have responsibilities in relation to collecting, storing and processing any personal data in accordance with this policy. Staff must only process personal data where it is necessary in order to do their jobs. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

Collecting personal data

The Charity will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law. We will only collect, use and otherwise handle your personal data where the individual has consented to this for specified reasons; where this is necessary to fulfil legal obligations or where it is necessary for our legitimate interests in running our organisation; as long as, in each case, these interests are in line with applicable law and your legal rights and freedoms. This includes:

- Complying with statutory registration requirements for Ofsted, Charities (Protection and Social Investment) Act 2016 and follow the recommendations of the official regulator of charities, the Charity Commission
- To process donations or other payments, to claim Gift Aid on donations and verify any financial transactions
- To provide services that have been requested.

- To update service users with important administrative messages about membership, events, services or payments
- To keep a record of our relationship with service users
- Processing payroll, pensions and expenses

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a child) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a child) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a service user that puts their safety, or the safety of our staff at risk
- Our suppliers or contractors need data to enable us to provide services to our staff and service users – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service
- We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our service users or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Charity holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

All subject access requests must be handled by the DPO. If staff receive a subject access request in any form they must immediately forward it to the DPO. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. However, it should be noted that a majority of our service users may be developmentally delayed and/or lack mental capacity, therefore this should be considered on a case-by-case basis as chronological age may not be an appropriate determining factor.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of an individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Individual Rights

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

CCTV

We use CCTV on our site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the DPO.

Photographs and videos

As part of our charitable activities, we may take photographs and record images of individuals within the organisation. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. We will not permit any photographs and videos to be taken by individuals outside of our staff team at our events for their own personal use.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used. We will obtain written consent from individuals aged 18 and over, for photographs and videos to be taken of them for communication, marketing and promotional materials.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on desks, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must declare this to the DPO
- Passwords that are at least 10 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices
- USB storage devices are not permitted
- Staff or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for charity-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of Data

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Charity's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The Charity will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the "Personal Data Breach Procedure set out at the end of this document. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Charity's processes make it necessary.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every 2 years and shared with the Board of Trustees.

HACS
Hillingdon Autistic Care & Support
Registered Charity Number 1066859

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

Responding to a Possible Personal Data Breach

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed or made available where it should not have been, made available to unauthorised people.
- The DPO will alert the CEO and the Board of Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality

- Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Charity's computer system
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- As above, any decision on whether to contact individuals will be documented by the DPO.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts relating to the breach
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

- The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

Ensure that any possibility of further data loss is removed or mitigated as far as possible.	Change passwords or access codes Isolate/close part of network Take down webpages Restrict access to systems to a small number of staff until more is known about the incident Consider additional physical measures that can temporarily be put in place
Determine whether anything can be done to recover any losses	Physical recovery of lost data/equipment – inform CEO/ Physical recovery of stolen data/equipment – inform CEO and the police as appropriate Use back-ups to recover corrupted data Recall incorrectly sent emails. If the recall is unsuccessful try contacting the person(s) to whom the data has been disclosed, apologising and asking them to delete the email from their systems (including from deleted items folders) and to confirm that they have done so Retrieve paper documents from any unintended recipients