CAPS Independent Advocacy

Data Protection Policy

Background

CAPS is committed to protecting the rights and privacy of individuals in accordance with our responsibilities under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

'Personal data' means information about living persons who can be identified directly from the information in question, or who can be indirectly identified from that information in combination with other information held about them. At CAPS, we use the terms 'personal information' and 'personal data' interchangeably.

We need certain personal information about our Management Committee members, personnel, volunteers, advocacy partners, participants and other contacts. Some information may be needed for administrative purposes, for example to pay staff wages. Other data may be needed for us to send information to people, such as meeting minutes or newsletters. Some information is necessary in order to effectively undertake our work, for example our advocacy partners' contact details and case notes.

This policy aims to ensure that CAPS complies with the UK General Data Protection Regulation and the Data Protection Act 2018 and that personal information about people is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This policy should be read in conjunction with CAPS' Confidentiality Policy, Schedule for Retaining Records, SAR Procedure, and if applicable, the relevant Code of Practice for handling data.

This policy will be reviewed annually to ensure it is kept up to date. Responsibility for reviewing this policy sits with CAPS' Data Protection Adviser.

Scope of policy

The policy applies to everyone who works with CAPS, including employees, sessional workers, consultants, volunteers, placement students, Management Committee members, and members of recruitment panels.
All these people will be expected to read and comply with this policy.

Policy Statement

Register of Fee Payers

The Data Protection (Charges and Information) Regulations 2018 requires every organisation that processes personal information to pay a fee to the Information Commissioner's Office (ICO) unless they are exempt. The ICO maintains a public register of such fee payers. People can consult the register via the ICO website to check an organisation is registered and the level of fee paid.
CAPS is a data controller and is registered with the ICO; registration number Z4982565.

The Data Protection Principles
CAPS guarantees that all processing of personal data will be done in accordance with the seven data protection principles as set out in Article 5 of the UK GDPR.

Principle 1 – Lawfulness, fairness and transparency:
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

This means:

- CAPS will only process personal information for an identified legal basis. The exact legal basis used will vary depending on the data processed and the area of our work it relates to;
- CAPS will only process special category personal information or criminal offence information where we have identified a condition to do so. See Appendix 1 (Processing Conditions) for more details;
- CAPS only processes personal information in ways people could reasonably expect;
- CAPS issues privacy statements in relation to all personal information processed which explains clearly what the data will be used for and how it will be handled. See section entitled 'Privacy Notices' for more information.

Principle 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.

This means:

- CAPS will explain what a person's personal information will be used for in our Privacy Notices and will not use it for any other purpose;
- CAPS will clearly identify and document our purposes for processing information;
- CAPS will consider data protection issues as part of the design and implementation of our work and will undertake such assessments as may be appropriate, for example Data Protection Impact Assessments (DPIA), Legitimate Interests Assessments (LIA).

Principle 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.

This means:

- CAPS will not collect any personal information that it doesn't need;
- CAPS will review the data it holds regularly and delete anything which is no longer necessary. See Appendix 2: Retaining and Disposing of Information.

Principle 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.

This means:

- CAPS will review and update information as necessary to ensure that information held is accurate and up-to-date;
- CAPS will carefully consider any challenges as to the accuracy of information held and rectify any information found to be inaccurate.

Principle 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.

CAPS will not keep personal information for longer than we need to. See Appendix 2: Retaining and Disposing of Information.

Principle 6 – Integrity and confidentiality (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.

This means:
- CAPS will ensure that we have the appropriate technical and organisational measures in place to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal information held;
- CAPS will ensure that personal information held will only be accessible to people who need to use it in the course of their work.

See Appendix 3: Security of Data for further details.

Principle 7 – Accountability:
The controller shall be responsible for, and be able to demonstrate compliance with these principles.

This means:
- CAPS understands and complies with the responsibilities it has in relation to people's personal information set out in the Data Protection Principles;
- CAPS has policies; procedures and recording systems in place to explain and evidence our compliance with these principles.

Data Protection Adviser
CAPS has appointed a Data Protection Adviser whose role is to provide advice and guidance to staff on all data protection issues. The Data Protection Adviser is also responsible for carrying out many of the data protection procedures detailed in this policy.

Currently, the Data Protection Adviser role is carried out by the Finance & Administration Manager.

Data Protection by design and default
CAPS is committed to the careful consideration of Data Protection and privacy issues both at the start of, and throughout, all the work we do.
An internal audit of all existing data and systems was undertaken in 2017 and all subsequent new projects, or changes to existing systems, must be assessed for any data protection implications. Staff involved in project design or development are

expected to liaise with Data Protection Adviser to ensure all possible data protection issues are fully assessed.
This will include identifying the legal basis for any new data processed, undertaking DPIAs or LIAs where appropriate, and fully assessing any proposed Data Processing Agreements or Data Sharing Agreements.

Privacy Notices
As part of our commitment to Principle 1 (lawfulness, fairness and transparency) and to individuals' right to be informed, we produce Privacy Notices in relation to all the personal information we process.

Which Privacy Notice applies to an individual will depend on the nature of their relationship with CAPS. Privacy Notices may be incorporated into forms at the point data is gathered, or into leaflets issued at the start of work with an advocacy partner. An up-to-date list of all Privacy Notices currently in use can be found in CAPS' Data Protection Manual.

Privacy Notices will explain what people can expect us to do with their data once we collect it. It will give details on what personal data we collect and what the legal basis for processing is, what we do with that data, who might see it and how long we keep it. Privacy Notices will also inform people as to their individual rights under the UK GDPR.

As far as possible, CAPS' Privacy Notices will be written in clear and concise language and will be easy to understand.

Rights of Individuals
The UK GDPR grants people certain rights regarding their personal information held by CAPS, including the right to be informed about what information we collect and why, the right to access information held by CAPS and the right to rectification if the information we hold is inaccurate.

CAPS is committed to upholding the rights of individuals both in our day to day practice and when designing our policies and procedures. The exact rights an individual has depends on the legal basis under which their personal information is being processed and are always explained in full on our Privacy Notices. Please refer to the appropriate CAPS Privacy Notice for more information on which rights apply in a particular circumstance.

More general information on the rights of individuals can be obtained from the ICO website: www.ico.org.uk.

Subject Access Requests
People have the right to access their personal information held by CAPS. Anyone who wishes to access their personal information held by CAPS should request this verbally or in writing. Such a request is known as a 'Subject Access Request' (SAR). Any such request will normally be granted within one month of receipt of the request. There is usually no charge for this service.

CAPS has a dedicated SAR procedure which sets out in more detail how SARs are handled. All staff should read and familiarise themselves with this document as a SAR could be made to any part of the organisation. Any member of staff receiving a SAR should direct this to the Data Protection Adviser straight away.

Data Processing Agreements
To enable us to carry out our work, we may contract with external organisations to process personal information on our behalf. Organisations that we enter into these arrangements with are known as data processors. Examples include CAPS' email service and cloud storage provider and the case management software in use in the Individual Advocacy service.

Where an external data processor is used, this will be with a formal Data Processing Agreement in place. CAPS will only enter into a Data Processing Agreement with organisations that implement appropriate organisational and technological measures to protect individuals' rights and comply with the data protection principles. Please see Appendix 3: Security of Data for further details.

Data Sharing Agreements
From time to time, CAPS may enter into Data Sharing Agreements with other organisations where this is required by the needs of the project. When considering whether to enter into a Data Sharing Agreement, CAPS will conduct a DPIA in order to fully consider any risks to the rights and freedoms of data subjects from the proposed agreement.

Personal Data Breaches
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

CAPS will take all reasonable steps to minimise the risk of data breach, for example through staff training, policy and procedure, and technical measures (as detailed in Appendix 3: Security of Data).

In the event that an actual or suspected data breach does occur, this must be reported to CAPS' Data Protection Adviser as soon as possible who will investigate the incident in co-ordination with CAPS' CEO.

The Data Protection Adviser will conduct a risk assessment to determine the potential adverse effect of the incident on the individual or individuals concerned. If the data breach is likely to have an impact on individuals' rights and freedoms, CAPS will notify the Information Commissioner's Office (ICO). The ICO must be notified of any reportable data breach within 72 hours.

In the event of a significant data breach CAPS will also inform the people whose data may have been affected, if known, and inform them of the measures we are taking to rectify the situation.

Disclosure to third parties
There are various reasons why CAPS might pass on personal information to someone outside of the organisation, depending on the situation.

The relevant Privacy Notice will always explain the **routine circumstances** in which we would pass on personal information and where to. For staff personal data, an example would be passing on information about earnings to HMRC. For our advocacy partners, examples include times when someone asks us to pass on their details, for example to assist them in accessing another service, or if we are obliged

to report a safeguarding concern under Adult Support and Protection or Child Protection legislation.

However we may also pass on personal data in other **urgent or exceptional circumstances**. Examples include:

- To comply with a court order;
- To protect public health, for example to comply with contact tracing during the coronavirus pandemic;
- When necessary to protect the health, safety and welfare of staff members, for example if a member of staff does not check in as expected when lone working;
- To prevent serious physical harm to a person;
- To protect someone's vital interests – this refers to life or death situations.

Wherever it is possible and reasonable to do so, CAPS commits to consulting an individual about the need to share their information in advance. However, the urgent or exceptional nature of the above circumstances means this may not always be possible.

Please refer to the following CAPS policies and procedures for further information and detailed guidance on the procedures staff must follow when disclosing personal data to third parties:

- Confidentiality Policy
- Personal Safety and Lone Working Policy
- Safeguarding Policy Statement
- Protection of Adults at Risk Policy
- Child Protection Policy
- Code of Practice relevant for each area of CAPS' work

Appendix 1: Processing Conditions

Principle 1 of the data protection principles states that personal data shall be processed fairly and lawfully, and in particular shall not be processed except for under an identified lawful basis. CAPS processes personal information under a variety of legal bases depending on the area of our work. A central record of the various legal bases we use to process data is kept in CAPS' Data Protection Manual.

Processing special category data and criminal offence data requires additional conditions are met, as described below. A central record of additional processing conditions is also kept in the CAPS Data Protection Manual.

Lawful bases

The lawful bases for processing information are set out in Article 6 of the UK GDPR. At least one of these must apply whenever CAPS processes personal data:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Special Category data

Special category data is personal information that needs more protection because it is sensitive. Examples of special category data that CAPS may hold include information about a person's health; racial or ethnic origin; political opinions; trade union membership; religious and philosophical belief; sex life or sexual orientation.

To process information of this type, CAPS must identify both a lawful basis as described above and a separate condition for processing this data under Article 9 of the UK GDPR.

A full list of the Article 9 processing conditions can be found on the ICO website. The Article 9 conditions used by CAPS are recorded in the CAPS Data Protection Manual.

Criminal offence data

Criminal offence data is personal information that needs more protection as it relates to criminal convictions and offences. This includes unproved allegations, and information relating to the victims and witnesses of crime.

To process information of this type, CAPS must identify both a lawful basis as described above and a separate condition for processing this data under Schedule 1 of the Data Protection Act 2018.

A full list of Schedule 1 processing conditions can be found on the ICO website. The specific Schedule 1 processing conditions used by CAPS are recorded in the CAPS Dara Protection Manual.

Appendix 2: Retaining and Disposing of Information

CAPS will not keep personal information for longer than we need to. Information will be kept according to CAPS' Schedule for Retaining Records.
Information will be disposed of in a way that protects the rights and privacy of data subjects, i.e. paper records will be shredded, electronic records will be erased.

Appendix 3: Security of Data

CAPS is committed to keeping the data we hold secure. As an independent advocacy organisation, we believe that trust and confidentiality are fundamental to our relationship with our advocacy partners.

Staff have a commitment to data protection and follow our Confidentiality Policy and the Code of Practice for handling data relevant to their area of work.

We take various measures to secure the personal data that we hold. The exact measures taken will depend on the format of the data and the area of work it relates to. Please refer to the Code of Practice for handling data for your area of work for more detail on data handling procedures. The following table contains a summary of measures taken and is non-exhaustive:

Type of information	**Measures taken**
Paper hard copy	• Personal information stored on paper is kept to the absolute minimum. Wherever possible, it should be anonymised. • Staff are advised to transfer personal information from paper onto electronic storage as quickly as possible and to securely dispose of the originals. • Any personal information that does require to be held on paper is stored securely in locked, non portable storage containers. • Access to storage containers is strictly limited to people who need to see the data in the course of their work.
Electronic – stored locally on CAPS devices	• All devices are password or PIN protected. Passwords/PINS are confidential; • Devices are not left switched on unattended without password/PIN protected screen-savers/locks; • Operating systems and software are kept up-to-date on all devices; • Firewalls and antivirus software are used on all computers and laptops; • Staff are advised not to download third party apps without checking with the Finance & Administration Manager;

	• Staff are advised to keep the use of USB drives and memory cards to a minimum, and to scan these with antivirus software before use; • Staff are advised not to keep personal data stored locally on devices longer than necessary and instead to use the cloud storage or case management software as appropriate to their area of work; • Staff are advised to never allow another person to use any of their devices; • Staff are advised to never access our systems using a non-CAPS device; • Staff are advised not to use public WiFi; • Staff are advised they should never take CAPS devices outside of the UK nor work remotely from outside of the UK; • all mobile phones can be tracked, locked and wiped remotely;
Electronic – stored remotely on cloud storage or case management software	• **Data transmission –** data in transmission is sent encrypted via Secure Sockets Layer (SSL) or Transport Layer Security (TLS); • Staff are advised to exclusively use cloud storage for the long term storage of personal data. This has the advantage of being physically separate from our office and stored in several different places to minimise the risk of data loss; • Exclusive use of cloud storage also means personal data can be managed and deleted centrally once it is no longer required; • User accounts can be suspended remotely if a particular device is lost or stolen; • User accounts are configured to automatically suspend in the event of suspicious activity, e.g. multiple failed log in attempts; • Storage and systems permissions are restricted to give staff only sufficient access needed to perform their role; • Staff are advised never to use personal email accounts or mobile phones to conduct CAPS work; • e-mail accounts are configured to filter out spam; • staff are advised not to interact with spam e-mail and to report potential phishing e-mails to the Finance & Administration Manager.

Appendix 4: Definitions

Data Controller
Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Processor
Any person (or organisation) who processes personal data on behalf of a data controller.

Personal Data
Information relating to a living individual who can be identified by the information or other information held by the data controller. This includes name, address, telephone number, expression of opinion about the person, and the intentions of the data controller in respect of the person.

Special Category Data
Relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, and sexual orientation. Special category Data also includes genetic and some biometric data. Special category data are subject to much stricter conditions of processing than other personal data (see Appendix 1).

Criminal Offence Data
Relates to information about criminal activity, allegations, investigations and proceedings. Also includes data about the lack of convictions or related to the victims or witnesses of crime, as well as data about penalties, restrictions or conditions placed on an individual as part of the criminal justice system. Criminal offence data are subject to much stricter conditions of processing than other personal data (see Appendix 1).

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data, disclosure or otherwise making available of data.

Third Party
Any individual or organisation other than the data subject, the data controller or its agents (including any relevant data processors).

This Data Protection Policy adopted by CAPS Management Committee on 27th May 2021. Reviewed June 2023 (KR)