**Data Protection Policy and Procedures**

Version Control:

|  |  |
| --- | --- |
| Last Reviewed and updated: | 13.04.23 |
| Next scheduled review (note may be reviewed sooner): | 14.04.24 |
| Owner: | Benjamin Napier, Chief Executive |

Policy and Privicy Statement:

**All data/information obtained, stored and processed by the organisation is covered by these policies and procedures.**

Citizens Advice Edinburgh recognises that the handling of identifiable, personal and sensitive information may be necessary for the effective functioning of the organisation and the services we provide. This may include information obtained from a 3rd party. Information may be held about individuals using and providing the organisation's services and about individuals in organisations we work in partnership with.

We all have a responsibility to protect the data we hold about people including how we process that data, whether that is citizens, volunteers, employees or partners. Our reputation as an organisation people can trust also depends on our ability to uphold and maintain data protection standards, in accordance with the law and best practice.

The main aims of this policy are to:

* Ensure that the organisation complies with the Data Protection Act 2018 and the associated Codes of Practice and Regulations (including the General Data Protection Regulation (GDPR).
* Ensure that information given in trust by users of the organisation services, our employees and volunteers or information that is held by the organisation for any other reason; is treated in compliance with the law and associated regulations.
* Ensure that information is protected in terms of how it is stored, processed and shared in compliance with the law and associated regulations.
* Ensure that the boundaries of confidentiality and individuals rights in relation to data protection are clear and understood by users of our service, our employees and our volunteers and that we are therefore confident that they are able to provide informed consent.
* Ensure users are aware of the organisation's responsibilities to protect, control, process and store their information, including requests for access.
* Make explicit the responsibilities of employees and volunteers concerning data protection, confidentiality and management of a Data Breach.
* Ensure that we remain compliant with Data Protection, including maintaining an up-to-date Data Asset Register, carrying out regular Data Protection Audits, providing continuing professional development for employees and volunteers and applying a Data Protection Impact Assessment to any new services or processes we undertake.

**Responsibility for the control of personal data:**

The organisation’s Data Protection Officer and Senior Information Risk Owner is the Chief Executive, who is responsible for ensuring all data is controlled in compliance with the Data Protection Act 2018 and associated Codes of Practice and Regulations. In accordance with our Data Protection Authorisation, the Scottish Association of Citizens Advice Bureau (Citizens Advice Scotland) is a Joint Data Controller. More information about their Data Protection Policies and Procedures can be found at [www.cas.org.uk](http://www.cas.org.uk)

**Information and Training:**

All employees and volunteers will be provided with this policy document and new employees and volunteers will receive a copy of this policy on taking up appointment.

All employees and volunteers **must** complete CASLearn online training on Data Protection. It is the responsibility of their line manager to ensure this has been completed. Completion of CASLearn provides the organisation with an audit trail that this standard of knowledge and understanding has been achieved for all employees and volunteers.

The organisation will provide continuing professional development on issues relating to confidentiality and the contents of this policy in order to ensure that our practices remain up to date and compliant.

Compliance with this policy is a condition of employment and/or continued volunteering and any deliberate breach of this policy will result in disciplinary action, which may include dismissal and possible legal action.

All staff and volunteers must sign their agreement to the Confidentiality and Data Protection Mandate.

**Principles:**

Everyone responsible for using data in the organisation has to understand and comply with Data Protection Legislation and associated regulations. They must make sure the information is:

•used fairly and lawfully

•used for limited, specifically stated purposes

•used in a way that is appropriate, relevant and not excessive

•accurate

•kept for no longer than is absolutely necessary

•handled according to people’s data protection rights

•kept safe and secure

•not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as:

•Age

•Gender

•Ethnic background

•Race

•political opinions

•religious beliefs

•health

•sexuality

•Commission or alleged commission of an offence

The principle of confidentiality runs through all of the organisations interactions with employees, volunteers and people who use or access our service. Information should only be shared when there is a clear and legal justification for doing so and where possible, with the informed consent of the individual involved.

Although personal/sensitive data is protected by the organisation, there are exceptional circumstances when confidential information would have to be disclosed in accordance with the Adult Support and Protection (Scotland) Act 2007, the Children (Scotland) Act 1995 and/or the Children and Young People (Scotland) Act 2014 and CAE’s related policy. In these circumstances, the CEO will make the final decision if personal/sensitive information should be disclosed. If the CEO is absent and not contactable, the Advice Services Manager or Project Manager will be authorised to share information where they believe that information needs to be disclosed in accordance with the legislation above and in accordance with CAE’s related policy and procedures.

**Confidentiality Policy**

Confidentiality is one of the fundamental principles of the CAB service. Citizens Advice Edinburgh assures confidentiality to all clients and nothing learned by bureaux from clients, including the fact of their contact(s) will be passed on to anyone outside the service without their consent. The services’ Data Protection Policy and Procedure contains details of the limits of how client’s data is recorded, stored and processed.

Confidential information will only be disclosed with client’s knowledge and informed consent or in accordance with a lawful basis under this Policy and Procedure, our Data Protection Policy and Procedure and/or if necessary, our Protecting Vulnerable Groups Policy and Procedure.

All employees and volunteers with access to client information must sign a Declaration of Confidentiality and Data Protection (appendix 1). Any person who has not signed the Declaration of Confidentiality and Data Protection should not have access to client identifiable information.

Where members of the management committee/Board require access to client information e.g. to investigate a complaint, a Declaration of Confidentiality must be signed, which will have a “limited life” of 3 months. This limitation exists to limit access to client records to that which is essential.

**Confidentiality Procedure**

1. All Citizens Advice Edinburgh staff, volunteers and Directors, must sign the Confidentiality and Data Protection Declaration. Any person who has not signed the Declaration of Confidentiality must **NOT** have access to information, which will enable a client to be identified without the informed consent of the client.
2. Whilst basic information may be asked for the purposes of triage at reception, the client will always be given the option to discuss information in private if they wish to do so. Clients must not be forced to state the nature of their enquiry in the presence of others.
3. Clients will be given the option of having their interview in aural privacy, but some contact may be better served in a more public contact area. The client will always be given the choice of how they wish to access their service.
4. No referrals will be made without the knowledge and informed consent of the client.
5. No information about a client will be given to a third party without the knowledge and informed consent of the client, unless, as stated above this is required in order to carry out our duties in accordance with our Supporting Vulnerable Groups Policy and Procedure and its related legal requirements.
6. Advisers should check with clients and record on the case record if the agree to the service making contact with them by phone or in print and record their reference, including clearly stating if no contact has been agreed.
7. Case records and case notes should only be removed from a designated service area in exceptional circumstances and only on the authorisation of the relevant manager and in accordance with our Data Protection Policy and Procedures.

**Procedure for any circumstance where Citizens Advice Edinburgh believe they may need to breach a client’s confidentiality:**

1. The decision to breach a client’s confidentiality can only be taken by a Manager. If a staff member or volunteer feels a breach of confidentiality may be necessary, they must consult their line manager before taking any further action. If the manager is not available, the consultation should be with the person nominated to be responsible in the manager's absence.
2. If the manager considers that a breach of confidentiality may be justified, they must agree this with the Chief Executive, unless this has been delegated to them in the Chief Executives absence. In any case, the manager will also discuss and agree this course of action with the Network Development Manager at Citizens Advice Scotland unless there is an urgent need to protect the safety and wellbeing of the client, in which case the Network Development Manager will be informed of the course of action and reasons thereafter.
3. Where a breach of confidentiality is agreed, reasons for the breach and specific details of the actions taken will be recorded on the client's file and unless there is a lawful basis not to do so, the client must be fully informed.

**Personal data regarding employees and volunteers:**

Personal data relating to employees or volunteers may be collected primarily for the purposes of:

* recruitment, promotion, training, redeployment, and/or career development;
* administration and payment of wages and sick pay;
* calculation of certain benefits including pensions;
* disciplinary or performance management purposes;
* performance review;
* recording of communication with employees, volunteers and their representatives;
* compliance with legislation, including data protection and related IT Security;
* provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers and;
* Staffing and volunteer levels and service planning.

The organisation considers that the following personal data falls within the categories set out above:

* Personal details including name, address, phone number, any health information required for reasonable adjustments or an individual’s safe care and protection, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
* References and CVs;
* Emergency contact details;
* Notes on discussions between management and the employee or volunteer;
* Appraisals, Supervision and Development Records and documents relating to grievance, discipline, promotion, demotion, or termination of employment or volunteering;
* Training records;
* Salary, benefits and bank/building society details; and
* Absence and sickness information.

Employees, volunteers or potential employees and volunteers will be advised of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed.

**Data Protection Procedure:**

**Data Asset Register:**

The Organisation will maintain a Data Asset Register which records a summary of all of the data the organisation holds, its purpose and location. This will be reviewed on a quarterly basis to monitor compliance with the law and associated regulations.

The Chief Executive will undertake an annual audit of the organisations compliance with this policy and procedure and report findings and any areas for improvement to the Board.

**Obtaining Informed Consent:**

All new service users will either be given a paper copy of the Data Protection Mandate (copy below) detailing their rights to Data Protection and explaining how and where we will store any information, they share with us, or they will have our privacy statement read out to them by phone and signposted to the Data Protection information on our website, or if contact is first being made on line; they will be signposted to our privacy statement and Data Protection Policy on the Website. They will be asked to confirm their understanding and agreement to the Data Protection Mandate, which will include a note recording any areas of potential information they have asked us not to record. When a paper record has been obtained, this information will be scanned and uploaded to their Case Record on CASTLE and the CASTLE Casenote will also confirm their informed consent has been obtained by that adviser. Thereafter, all information relating to that contact with the service user will be managed in accordance with that agreement.

Where an existing or previous service user asks for advice in relation to another matter that requires them to share new personal or sensitive information, it is imperative that the adviser re-confirms the clients understanding and agreement to the Data Protection Mandate and obtain specific consent for the management of that new information.

If a client has been referred to Citizens Advice Edinburgh from one of our National Helplines, the above process must be completed again by the Citizens Advice Edinburgh Adviser, to ensure consistency and compliance with our own data protection requirements.

Employees and volunteers will be given a personal annual reminder of the information that we hold on their HR record and asked to provide their consent to this information being maintained.

Posters will be displayed in our Bureau and any other location where we are providing a service (unless we are unable to do so) which remind users of our service about their rights to Data Protection (copy below). This information will also be available and promoted through our website, with regular reminders posted through our social media.

**Circumstances in which we might use someone’s information without their permission or consent:**

In very specific circumstances, we might need to use or share your information without your permission. If we do, we will always make sure there's a **lawful basis** for it. Examples of these circumstances include:

* to comply with the law, called **'legal obligation'** - for example, if a court orders us to share information
* to protect someone's life, called **'vital interests'** - for example, sharing information with a paramedic if a client was unwell at the bureau or one of our outreaches
* to carry out a contract we have with you, called **'contract'** - for example, if you're an employee we might need to store your bank details so we can pay you
* to defend our **legal rights** - for example, to resolve a complaint that we gave the wrong advice

**Requests for access to or amendment of data (Subject Access) Request:**

If an existing service user asks for access to any personal or sensitive information or for that information to be amended or removed from our records, in accordance with their legal rights, they should be given the “Data Protection (Subject Access) Request” (copy below) to complete and this must be passed onto the bureau manager and to the CEO for action. An employee or volunteer can make a request at any time directly to their line manger to see their HR Record. In both circumstances, information should be provided within 30 calendar days of the request being made.

Any request for deletion or amendment of records will also have to be risk assessed for insurance purposes and if we believe there is a risk to the organisation whereby we may need to defend our legal rights, we may not be able to delete or amend a record. In such circumstances the client will be fully advised on that outcome.

**Storage and Disposal of Information:**

All information we obtain about users of our service will only be stored on our electronic data base CASTLE.

Employees of CAS or other Citizens Advice Bureaux in Scotland may access this record, where necessary, in order to provide advice seamlessly across the Scottish network of Citizens Advice Bureaux.

Some of our services are also subject to external audit by the Scottish Legal Aid Board (SLAB). They check that we are providing you with the highest quality of service and are allowed to access your information for audit and quality assurance purposes only, under the legal basis of ‘public task’.

In some circumstances, temporary paper records will also need to be kept for Case Managed Contacts and Tribunal Representation, where access to paper records are required for purposes of the service we provide. These paper records will be scanned onto CASTLE once access to the paper record is no longer necessary and the paper record will be destroyed. In circumstances where that paper record is extensive and it is not practical or efficient to scan all of the documentation to CASTLE, a paper record may be maintained and will be held securely for the same duration as the CASTLE Record. In these circumstances, an alert will be added to the CASTLE record, so that any paper record will be directly connected to it.

We may record information on a note pad during an interview, but this information will be transferred onto CASTLE within 28 days and the paper record destroyed.

Where a service user shares personal or sensitive information with us in paper form (which is not a Case Managed Contact or for a Tribunal Representation) and it is necessary for us to keep a record of that information, this will be scanned onto CASTLE and the paper record either returned to the service user or destroyed within 28 days.

If we are required to produce any other record on paper that will be scanned to CASTLE within 28 days and the paper record destroyed.

Where a paper record is maintained, that record will be held in a secure and lockable storage facility accessible only to designated representatives of CAE. In certain circumstances an Adviser may be required to transport paper records out with the organisations premises, this may be for purposes of attending a tribunal, meeting a client in another service or home visit, or transferring files from one location to another. CAE recognise that this may be necessary for the services we provide and that during such circumstances we cannot provide the same level of security. Advisers must therefore only transport information when it is absolutely necessary and only the information that is required for that purpose.

It is the responsibility of the organisation’s employees and volunteers who are handling that data to ensure that personal/sensitive information about service users (individual clients, members, groups and organisations) is treated as confidential and stored securely in accordance with the details above.

The organisation uses the services of an external confidential waste collection agency and has monitored their policy for compliance with Data Protection Legislation and associated Regulations.

**If you browse our website:**

When you browse our website, we collect 'cookies' to help us understand more about how our site is used by visitors, and to develop and enhance our services to you.

A 'cookie' is a bit of information kept on your computer. It tells us things like what device you're using and what pages you click on.

We use cookies to:

* track aspects of user visits, including the length of a user's visit, their browser, geographic location and the use of the search facility on this website
* **Please note** - If you use our **Chat** function, we will be collecting and processing different data about you and specific privacy policies and data protection rules apply to this service. For those specific details, please see appendix 1 below.

**Telephone Calls and Letters:**

Any mail we receive in relation to a client, will either be scanned immediately onto CASTLE or stored in a secure and locked cabinet until it is transferred onto CASTLE and the paper record subsequently destroyed within 28 days.

Access to a room where phone calls can be made in private will be available to employees and volunteers working in open plan offices.

**Other Platforms Used to help you reach and engage with our Services:**

If you contact us by phone:

We use a company called Soho 66 as our phone provider. If you phone us, a record of your phone number will be available on our secure online customer portal which can only be accessed by a secure user name and password and is only accessed by our Management Team. More details about Soho 66 data protection and privacy policy can be found here:

[https://soho66.co.ukPrivacy-Policy.](https://soho66.co.uk/104383/all/1/Privacy-Policy.aspx)

If you make an appointment to see us:

We use an online appointment system called 10to8. If you make an appointment with us, we will record details of your name, date of birth, phone number and e-mail address, as well as a brief note about the nature of your enquiry if known (for example “help with benefits application”). This information can only be accessed by users authorised by Citizens Advice Edinburgh Management team and accessed by a secure user name and password. More details about 10to8 data protection and privacy policy can be found here:

[https://10to8.comPrivacy Policy](https://10to8.com/legal/#tabs|3)

If you contact us via one of our Social Media Platforms or Chose to share personal information on the comments section:

We do not seek to engage with clients using our Social Media Platforms. Instead, these are intended for raising awareness of our services and impact. However, we recognise that people may seek to engage with us using the comments or messaging services. If personal information is shared on these platforms, we will seek your agreement to transfer it to our CASTLE system and engage with you by phone, e-mail or in a direct meeting and we will delete your comments and personal information from our social media platform.

Every effort will be made to keep a track of such information, but we cannot guarantee that we will see every comment. Therefore, we strongly discourage any personal information being shared on these platforms and advise you to read their Data Protection and Privacy Statements here. If you are concerned that your data has been stored on our social media, please contact us on 0131 510 5510 so that we can seek to remove that on your behalf.

[https://gdpr.twitter.comGDPR HUB](https://gdpr.twitter.com/en.html)

[https://www.facebook.comGDPR HUB](https://www.facebook.com/business/gdpr)

[https://privacy.linkedin.comGDPRHUB](https://privacy.linkedin.com/gdpr)

E-mail and other Microsoft products we use to communicate with you and other third parties:

We use Microsoft Office as the platform to host our e-mail, word and other Microsoft tools. Your personal data may be recorded in e-mail communication with you and any third party you have agreed for us to contact and a record of correspondence drafted in word or details recorded on excel may be retained within our Microsoft documents portal. Every effort will be made to delete such documents once they have been scanned and uploaded to CASTLE, but given the volume, some may remain within our Microsoft portal. Such information can only be accessed by users authorised by Citizens Advice Edinburgh Management team and accessed by a secure user name and password. More details about Microsoft Office data protection and privacy policy can be found here:

[https://www.microsoft.comGDPR](https://www.microsoft.com/en-gb/trust-center/privacy/gdpr-overview)

If we engage with you via Zoom or Microsoft Teams:

You may agree to engage with your adviser by video link using Zoom or Teams. If you do, those platforms may retain details of your name and e-mail address. More details about their data protection and privacy policies can be found here:

[https://zoom.usEuropean Data Protection Policy](https://explore.zoom.us/en/gdpr/)

[https://www.microsoftteams.comGDPR](https://www.microsoft.com/en-gb/trust-center/privacy/gdpr-overview)

If you provide feedback using our Citizens Advice Edinburgh Feedback Survey Link:

All clients will be invited to complete our online feedback survey. We use [SurveyMonkey UK](https://www.surveymonkey.co.uk/welcome/sem/?program=7013A000000mweBQAQ&utm_bu=CR&utm_campaign=71700000061148706&utm_adgroup=58700005508347663&utm_content=43700050331899354&utm_medium=cpc&utm_source=bing&utm_term=p50331899354&utm_kxconfid=s4bvpi0ju&gclid=3da95a2df3ee1f8897ae3e15f6ee4d11&gclsrc=3p.ds&msclkid=3da95a2df3ee1f8897ae3e15f6ee4d11) as the platform for this. If you chose to complete that survey, you must be aware of the Data Protection and Privacy Statement used by that provider. Details can be found here:

[Privacy Notice | Survey Monkey UK](https://www.surveymonkey.co.uk/mp/legal/privacy/)

[GDPR and CCPA Compliance | SurveyMonkey UK](https://www.surveymonkey.co.uk/mp/privacy/)

**Retention of Personnel Records:**

|  |  |
| --- | --- |
| **Document** | **Retention period** |
| Application form | Duration of employment or volunteering |
| References received | Duration of employment or volunteering |
| Annual appraisal/assessment/supervision /Training records | Duration of employment or volunteering |
| Annual leave records | For the leave period |
| Unpaid leave/special leave records | 3 years |
| Sickness records | 3 years |
| Records relating to accident or injury at work | For at least 3 years from the date the report was made |
| Disciplinary matters | 6 years |
| Payroll and wage information | 6 years |
| References given/information to enable references to be provided, e.g Summary of record of service, name, position held, dates of employment or volunteering | 6 years from reference/end of employment or volunteering |

**Data Breach:**

All employees and volunteers have a responsibility to take action where they think there may have been a breach of data protection. This will be any situation where a person’s data has not been managed in accordance with the above policy and procedure. If you think there may have been a breach you **must** report this immediately to your line manager or in their absence a member of the Senior Management Team and the CEO must be informed within 24 hours. We have a legal duty to report any breach of Data Protection to the Information Commissioners Office within 72 hours, therefore immediate action must be taken by all employees and volunteers if they have any concern that a breach may have occurred. The CEO (alongside delegated responsibility to an appropriate member of the management team) will take responsibility for management of the data breach and reporting to CAS and the ICO in accordance with our legal and regulatory requirements.

A breach of data protection must also be recorded on CAE’s Incident Report and these will be recorded and reviewed for learning and development in accordance with our Incident Reporting processes.

**Citizens Advice Edinburgh**

**Confidentiality and Data Protection Declaration**

Confidentiality is one of the fundamental principles of the CAB service. Citizens Advice Edinburgh assures confidentiality to all clients and nothing learned by bureaux from clients, including the fact of their contact(s) will be passed on to anyone outside the service without their consent. The services’ Data Protection Policy and Procedure contains details of the limits of how client’s data is recorded, stored and processed.

Confidential information will only be disclosed with client’s knowledge and informed consent or in accordance with a lawful basis under our Data Protection Policy and Procedure and/or if necessary, our Protecting Vulnerable Groups Policy and Procedure.

All employees and volunteers with access to client information must sign this Declaration of Confidentiality and Data Protection. Any person who has not signed the Declaration of Confidentiality and Data Protection should not have access to client identifiable information.

Where members of the management committee/Board require access to client information e.g. to investigate a complaint, a Declaration of Confidentiality must be signed, which will have a “limited life” of 3 months. This limitation exists to limit access to client records to that which is essential.

I hereby confirm that I have read and understood this declaration and the associated policy and procedure it references and agree to uphold my responsibilities in accordance with them.

Signed:

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Print Name | Signature | Date: |
| Staff Member/Volunteer |  |  |  |
| Line Manager or CEO |  |  |  |

|  |
| --- |
| **\*\*\*DATA PROTECTION AUTHORISATION - YOUR LEGAL RIGHTS\*\*\*** |
| **It is important that you read and consider the information below carefully before giving us authorisation to manage and process your data.** |
| The Data Protection Act 2018 and the General Data Protection Regulation (**GDPR**) establish your legal right to control: what information you chose to share with us; how we use and process that information and; what information you chose to have on record. Citizens Advice Edinburgh will take responsibility for ensuring that any data you share with us is kept safe and secure and is held for no longer than is absolutely necessary.  In order to provide you with the best possible service, we will ask you to share personal and sometimes sensitive information, so that we have a good understanding of your circumstances and can give you the right advice. We will also maintain a record of your contact, which may contain sensitive personal data, often referred to as “Special Category Data”.  **Sensitive personal data** includes information relating to**:** race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, genetics, biometric data (where used for identification purposes) sexuality, commission or alleged commission of an offence or anything else you consider to be particularly sensitive. |
| **Citizens Advice Edinburgh will use your data for 2 purposes:**   1. To provide you with the advice and information you require at your chosen point of contact and for the organisation and our external auditors to undertake quality assurance of that advice, including asking for your feedback on our services. 2. To monitor the issues that are impacting on the lives of people locally and lobby for changes to legislation and social policy that will improve people’s circumstances and help address common problems.   For these purposes: The Scottish Association of Citizens Advice Bureau (Citizens Advice Scotland) and its members and; the Scottish National Standards for Information and Advice Providers Auditors, will also have access to this information. CAS will be a joint Data Controller.  Some personal information may also be held by platforms we use to help you engage with our services. For more details, please refer to our Data Protection Policy and Procedure at [www.citizensadviceedinburgh.org.uk](http://www.citizensadviceedinburgh.org.uk)  You can ask to see your records at any time and you can ask that we destroy your records if you no longer want us to hold that information. Otherwise, we will retain your records for no more than 7 years and only for the purposes outlined above. By law, we would have to establish a specific lawful basis, if we needed to retain your records for any longer. |
| **I give my** **explicit and informed consent to Citizens Advice Edinburgh (CAE) and Citizens Advice Scotland maintaining a record of my contact, including any sensitive data. I consent that they can destroy my file 7 years after my last contact.**  Clients Signature……………………………………………………………………… Date……………………….. |
| **If you do not agree to sign this Data Protection Mandate or if you have any questions before doing so, please speak to your adviser** |
| **Authorising a 3rd party to act on your behalf.**  If you wish someone to deal with your enquiry on your behalf, we need you to provide specific additional consent for that to happen. You must provide the name and contact details of the person(s) you authorise us to speak to on your behalf and state the particular issues we are authorised to discuss. This will allow us to discuss that information with this third party, but only you will control how we use and process that information in accordance with your data protection authorisation above.  If you do not require this level of assistance, then please do not complete this section:  I authorise (name of person/s)……………………......................................................................................  Who can be contacted at (address and/or phone number)…………………………………………………………….  ……………………………………………………………………………………………………………………………………………………….  To act on my behalf for issues concerning (please state):  ………………………………………………………………………………………………………………………………………………………..  ………………………………………………………………………………………………………………………………………………………..  ………………………………………………………………………………………………………………………………………………………..  Client signature………………………………………… Date………………….. |
| **For more information about our Data Protection Policy visit** [www.citizensadviceedinburgh.org.uk](http://www.citizensadviceedinburgh.org.uk) |

Appendix 1

**If you use our Chat Function on the Website:**

Citizens Advice Edinburgh is the controller and responsible for your personal data and it is a member of the Scottish Association of Citizens Advice Bureau (“Cas”), details of which can be found on its [website privacy policy](https://www.cas.org.uk/system/files/privacy_notice_-_general_for_website_0.pdf) (collectively referred to as "we", "our", "us" or "Cab").  This Privacy Notice sets out the type of personal information we collect about you, why we collect it, and how we use it when you use our chatbot service.

It is important that you read this Privacy Notice together with the rest of the policy and procedure outlined above which contains more detailed information about our data processing and can be accessed here or you can request a copy from us.

If you have any queries about our privacy practices or about this Privacy Notice contact us:

Address: For the Attention of the Data Controller, Citizens Advice Edinburgh, 58 Dundas Street, Edinburgh, EH3 6QZ

**What Personal Data we collect and how this is collected**

We collect personal data such as your phone number and information you provide us within the free text facility within the chat.

**Purposes of using your Personal Data and lawful basis we rely on**

We use your personal data to:

* provide you with the chatbot service and learn from and improve the service
* share the data with Cas to facilitate improvement of services and wider development of services for fellow members of shared services
* manage our relationship with you e.g. to contact you where you request this
* meet our regulatory requirements or legal responsibilities, as required.

We will only use your personal data when the law allows us to. Our lawful basis to process your personal data is in our legitimate interests. It is in our legitimate interest to respond to enquiries, requests, and information received to ensure we provide you with the relevant support, improve the service and share personal data with Google Cloud which helps us to provide the service.

**Who do you share my information with?**

We may share your personal data with Cas, our third-party supplier who helps us supply the chatbot service, and other local Citizen's Advice Bureaus to provide you with the correct advice and/ or support. We also share this data with Google Cloud, insurers, and regulators.

**International Transfers**

We transfer, store, and process your personal data outside the European Economic Area ("EEA") to the US via the use of [Google Cloud using legally-provided mechanisms](https://cloud.google.com/privacy/gdpr) to lawfully transfer data across borders.

We transfer personal data to and from the EEA and UK based on the adequacy decisions for the UK and EU.

**How long do we keep records for?**

We will only keep your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including to satisfy any legal, insurance, regulatory, tax, accounting, or reporting requirements or if there’s a complaint or if we reasonably believe there is a prospect of litigation.

If you chose not to get in touch with us after the chat has ended we’ll keep the data from the chat for 3 months. Where you get in touch with us we keep this for 7 years and for certain complex cases we keep this data for 16 years.

We may keep data longer than these periods if necessary. Examples of where records need to be kept beyond the retention periods include records of advice and support around statutory debt options and building works over a certain value.

**Your Legal Rights**

Under certain circumstances, you have rights under data protection laws concerning your personal data including the right to receive a copy of the personal data we hold about you, the right to rectification, restriction, erasure, objection, as well as the right to portability. You also have the right to make a complaint at any time to a supervisory authority which is the Information Commissioner's Office in the UK and is the regulator for data protection issues ([www.ico.org.uk](http://www.ico.org.uk)).

|  |  |
| --- | --- |
| [Citizens Advice Edinburgh](http://www.citizensadviceedinburgh.org.uk/) | ***Data Protection***  ***Know Your Rights*** |

**In order to provide you with the best possible service, we will ask you to share personal and sometimes sensitive information, so that we have a good understanding of your circumstances and can give you the right advice.**

**You have the right to choose what information you share with us, what information you want us to record and to understand exactly what we are using that information for. You can ask to see or amend that information at any time and we will make the necessary arrangements to do that.**

**THIS IS YOUR LEGAL RIGHT**

**If you have any questions about the information we are asking for, why we are asking for it or how and where it will be stored and recorded, please ask your adviser or ask to speak to your Adviser**

**Further details about our Data Protection Policy can also be found at our website**

[**www.citizensadviceedinburgh.org.uk**](http://www.citizensadviceedinburgh.org.uk)

|  |  |
| --- | --- |
| [Citizens Advice Edinburgh](http://www.citizensadviceedinburgh.org.uk/) | ***Data Protection (Subject Access) Request*** |

Request to access, amend or remove personal or sensitive information mandate

**To the Chief Executive of Citizens Advice Edinburgh:**

I hereby request (please select the relevant option):

|  |  |
| --- | --- |
| A copy of all information that Citizens Advice Edinburgh has recorded about me |  |
| That Citizens Advice Edinburgh amend personal or sensitive they have recorded about me |  |
| That Citizens Advice Edinburgh remove (delete) personal or sensitive they have recorded about me |  |

I understand that I will need to present evidence of my identity that confirms my right to access that particular record. This will include photographic ID (either a Passport or Driving Licence) and confirmation of the address that the record is linked to in my name (either a bank statement, utility bill, payslip or letter from the DWP). I also understand that CAE will take no more than 30 days to respond to my request and that they may wish to discuss with me the best way to comply with my request and/or any other details about my request.

Name (Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Address (Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Postcode \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**For CAE**

I certify that I confirmed the identity of the client in accordance with the above identification requirements.

Name (Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Role (Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_