homemaker southwest
preventing homelessness, promoting independence

PRIVACY POLICY (DATA PROTECTION)

1. Why this policy exists

This privacy policy ensures Homemaker Southwest:

- protects the rights of individuals
- is open about how it stores and processes information about individuals
- reduces the risk of accidentally releasing data about individuals inappropriately
- complies with data protection law

2. Some basic definitions

- Personal Data - any information related to a living individual or 'Data Subject', that can be used to directly or indirectly identify the individual
- Data Subject - a living individual whose personal data is processed by a controller or processor
- Data Controller - the entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- Data Processor - the entity that processes data on behalf of the Data Controller

3. Scope

This policy applies to:

- All staff, trustees and volunteers of Homemaker
- All funders, contractors, suppliers and other people working with Homemaker

It applies to all data that the charity holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation (GDPR).

4. Policy Dissemination & Enforcement

Homemaker's Management Team is responsible for making sure that all staff and volunteers are aware of and comply with the contents of this policy

In addition, Homemaker will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) comply with the contents of this policy.

5. Legal basis for using personal data

At least one of the following conditions will apply whenever Homemaker processes personal data:

1. Consent: We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. Contract: The processing is necessary to fulfil or prepare a contract for the individual.
3. Legal obligation: We have a legal obligation to process the data (excluding a contract).
4. Vital interests: Processing the data is necessary to protect a person's life or in a medical situation.
5. Public function: Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
6. Legitimate interest: The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

6. The Data Protection Principles

Homemaker will comply with the data protection principles set out under the General Data Protection Regulation, as implemented on 25th May 2018. The Principles are:

1. Lawful, fair and transparent: Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. Limited for its purpose: Data can only be collected for a specific purpose.
3. Data minimisation: Any data collected must be necessary and not excessive for its purpose.
4. Accurate: The data we hold must be accurate and kept up to date.
5. Retention: We cannot store data longer than necessary.
6. Integrity and confidentiality: The data we hold must be kept safe and secure.

7. Accountability and Transparency

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation.

8. Data Security

We keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, Homemaker will first establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

9. The Rights of Individuals

Below is a list of the rights that a person has under data protection law. Some of the rights are complex, and not all the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities (ICO) for a full explanation of these rights.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

10. Data Protection Procedures

All new staff, volunteers and trustees will be asked to sign a Confidentiality Agreement which states they agree to follow Homemaker's Confidentiality Policy, this Privacy Policy and the ICT Systems Policy.

These procedures should be read in conjunction with all Homemaker's policies, which can be found on the website – www.homemakersw.org.uk

Andrea Carlisle is the Data Protection Lead.

11. Consent

Before we take any personal data from a client, we will first obtain the client's consent. This is requested and given verbally when a client telephones the agency, and followed up at the initial appointment by them signing a data protection statement which details how their data may be used, and a tick box for agreeing to be contacted for Research and Evaluation.

12. Storing data

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained.

- All client files are stored electronically on our case management system - Advice Pro.
- Paper files are stored in locked filing cabinets at Homemaker's offices in Exeter and Plymouth, and in commercial secure archive storage
- All employees will maintain a 'clear desk'
- Staff will use strong passwords which are set to be changed regularly

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

13. Destroying data

- Printed data will be shredded when it is no longer needed
- All files are stored in a secure storage facility for 6 years from the calendar year in which they are closed, unless the complexity or nature of the case requires that the files in held for longer. In this case permission will be sought from the client and the file will be clearly marked to prevent destruction. After 6 years files will be securely shredded.
- Records held electronically on Advice Pro are automatically deleted after six years
- Confidential waste bins are provided in the offices for the collection and subsequent shredding/destruction of confidential documents
- Commercial confidential shredding also takes place from the secure archive
- All staff are responsible for making sure that personal data is shredded
- Homemaker will ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party or destroyed.

14. Taking personal data out of the office

When taking personal and/or confidential data, in any format out of Homemaker premises – e.g. working from home, a home visit or outreach appointment, it is essential that the data is secure. Laptops will be securely password protected and only the client file necessary for the visit should be taken.

15. Transferring data internationally

There are restrictions on international transfers of personal data. We will not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission.

16. Subject access request (SAR)

Under GDPR, individuals can make a Subject Access Request in writing, to be:

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- Given a copy of the information comprising the data
- Given details of the source of the data (where this is available)

Homemaker's steps for conducting a Subject Access Request can be seen in Annex 1

17. Disclosure of personal information

All staff and volunteers, including the Trustees, should be familiar with the Confidentiality Policy, which sets out Homemaker's commitment to good practice in handling personal information.

- Data protection checks must be completed before giving any information over the telephone. This involves asking security questions: Name; DOB; National Insurance Number; First line of address & Postcode.
- If individuals or other agencies contact Homemaker in connection with a client, no information should be given without the client's permission. The permission should be in writing.
- If a client arranges to collect her/his file, we need a signed receipt for our records. A copy of all information given to the client should be kept at Homemaker.
- If an enquiry is made by phone, or in person, ask the enquirer to leave contact details and contact them when you have confirmed that they are entitled to the information. Don't confirm that the person they are asking about is a Homemaker client.
- If the enquirer has correspondence from Homemaker, they will have a caseworker reference. The enquiry should be passed on and the caseworker can decide whether it is appropriate to disclose the information.

- Staff addresses, and other contact details are held in a secure OneDrive work-space, which only the Management Team can access. These details must not be given to anyone outside Homemaker without the permission of the staff member. If the worker is not in the office, take details then contact the staff member and ask them to get in touch with the enquirer.
- If there is any doubt about disclosure, consult with either Director. There may be occasions when it is in the interest of the client or staff member to disclose information and the procedures are not intended to be obstructive or over cautious.
- Personnel information will not be disclosed unless there are exceptional circumstances e.g. where use of alcohol and/or drugs has become a matter for disciplinary proceedings; where an individual worker has had an accident and is not able to self-disclose medical conditions/allergies etc. This decision will usually be made by the Manager.

18. Employee Data

Homemaker collects and processes personal data relating to its employees to manage the employment relationship. Homemaker is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations. Homemaker collects this information in a variety of ways. For example, data is collected through application forms; from forms completed by employees at the start of or during employment (such as benefit nomination forms); or through interviews, meetings or other assessments.

In some cases, Homemaker collects personal data about employees from third parties, such as references supplied by former employers and information from criminal records checks permitted by law. Homemaker seeks information from third parties with consent only. Data is stored in a range of different places, including in your personnel file, in Homemaker's HR management systems and in other IT systems (including Homemaker's email system).

Homemaker needs to process data to enter into an employment contract, and to meet its obligations under that employment contract. In some cases, Homemaker needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

All employees, volunteers and trustees are issued with a copy of Homemaker's Employee Privacy Notice, along with a copy of the data held on them. This is reviewed annually to ensure accuracy.

19. Access

Personnel files are held in a locked filing cabinet, to which only the management team have access. Information is also stored within a secure OneDrive workspace.

20. Personnel file destruction

Homemaker will follow the Information Commissioner's Code of Practice on employment records.
Personnel files are destroyed securely six years after the worker leaves Homemaker. Prior to this they are stored separately in a locked filing cabinet, to which only the Directors have access, with the date for destruction marked on them.

21. Complaints handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Information Commissioner's Office. An investigation of the complaint will be carried out in the extent that is appropriate based on the merits of the specific case. Information Commissioner's Office will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Information Commissioner's Office, then the Data Subject may, at their option, seek to redress

through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office within the applicable jurisdiction.

22. Data Breaches

The GDPR introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to cause a high risk of adversely affecting the rights and freedoms of individuals, they must be notified.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material, or as part of a pattern of failures

23. Failure to Comply

We take compliance with this policy very seriously. Failure to comply puts both the individual and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If an individual has any questions or concerns about anything in this policy, they should contact a manager for advice

To ensure that all the principles included in GDPR are followed, Homemaker is registered with the Information Commissioner's Office with the number Z1165305

Document control

Ownership:	Homemaker Southwest
Date Issued:	July 2018
Governance Forum responsible	Trustee Board
Version:	July 2018
Document history:	July 2019 – updated /reviewed Jan 2020 – wording in section 22 amended.
Distribution	Website /One Drive
Next Review Date of policy:	July 2021
Review frequency	Annually

APPENDIX 1

SUBJECT ACCESS REQUEST

Clients and staff have the right to ask to see personal and sensitive information held about them by Homemaker, and the organisation would wish to respond positively.

The following checklist suggests how such requests should be handled.

- The request must be made either verbally or in writing by the individual concerned.
- The request may be made to a caseworker or to a manager.
- The Director should be informed of any such request, and the Line Manager given the task of preparing the information for disclosure.
- If the request is reasonable, the file should normally be available to view within 10 working days. The individual should be notified accordingly.
- If there is third-party information contained within the file, this should not be disclosed without the third-party's consent.
- The Line Manager should contact the third party to ask whether they will give their consent to disclosing the information on file. The response should be in writing wherever possible.
- The file should be sorted to take out third-party information if applicable.
- The individual making the request should be invited to the office to view the file in a private room.
- Where no consent has been given for third-party information to be disclosed, the individual should be made aware of this, and may be encouraged to contact the third party direct to follow this up if appropriate.
- A note should be made on file to say that the individual had access to their file, and the date recorded.