Privacy Policy

1 Why this policy exists

This privacy policy ensures Talking Money:

- 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

[more detailed definitions are shown in Annex 1]

3 Scope

This policy applies to:

All staff and volunteers of Talking Money

All funders, contractors, suppliers and other people working with Talking Money

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

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

In addition, Talking Money 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 Talking Money 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.

See Annex 2 for our legal bases for using personal data in more detail

6 The Data Protection Principles

Talking Money will comply with the data protection principles set out under the General Data Protection Regulation. 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. A privacy notice for clients, staff and members of the public can be found in ANNEX 3.

8 Privacy by Design

"Privacy by design" is an approach to projects that promotes privacy and data protection compliance from the start. Talking Money will ensure that all data security processes and IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

We will ensure that a Data Protection Impact Assessment (DPIA) is conducted, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Leadership Team for review and approval. Where applicable, the Information Technology (IT) provider, as part of its IT system and application design review process, will cooperate with the ICO to assess the impact of any new technology uses on the security of Personal Data.

9 Data Security

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

10 The Rights of Individuals

Below is a list of the rights that a person has under data protection law. See Annex 4 for summary of each. Some of the rights are complex, and not all of 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.

11 Data Protection Procedures

All new staff, volunteers and trustees will be asked to sign a Confidentiality Agreement which states they agree to follow Talking Money's Confidentiality Policy, this Privacy Policy and IT Acceptable Use Policy.

These procedures should be read in conjunction with the Information Security and Risk Management Policy, and the IT Acceptable Use Policy held within the Staff Handbook.

The Chief Executive is the Data Controller.

12 Consent

Before we take any personal data from a client, we will first obtain the client's consent. This is done through 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. See Annex 5 for the full data protection statement.

13 Storing data

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

- All client files are stored electronically on our case management system - Advice Pro.
- Paper closed files are all stored at Talking Money's main offices in Bristol BS2 and in commercial secure archives
- All employees will maintain a 'clear desk'
- Staff will use strong passwords which are set to be changed regularly

- The network drive is backed up every day – anything stored on a local hard drive will not be backed up and may be lost
- All servers containing sensitive data are approved and protected by security software
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

14 Destroying data

- Printed data will be shredded when it is no longer needed
- Client files will be deleted from the network drive when the paper file is destroyed i.e. After the file has been closed for six years
- Files can be deleted sooner than 6 years if an electronic copy of all relevant information is stored on the client's file
- Records held electronically on Advice Pro are automatically deleted after six years
- Confidential waste bins are provided in the main office for the collection and subsequent shredding/destruction of confidential documents
- Commercial confidential shredding also takes place from the secure archive
- Documents within the building will be shredded as soon as possible
- All staff are responsible for making sure that personal data is shredded
- All staff will be responsible for deleting 'closed' folders and confidential information on the network drive as soon as possible or when the files for the relevant year are destroyed

15 Taking personal data out of the office

Personal and/or confidential data, in any format, should not be taken out of Talking Money routinely but there will be occasions when it is necessary – e.g. working from home, seeing clients outside Talking Money – home, hospital, outreach, etc.

ki

When it is necessary to take personal information out of Talking Money it is essential that the data is secure.

1. To minimise the amount of information leaving the building, employees and volunteers will consider whether it is necessary to take a whole file or whether a few relevant pages would be enough.
2. If the file is taken on a laptop or a memory stick employees and volunteers will make sure it is password protected.

16 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.

17 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)

Talking Money's 5 steps for conducting a Subject Access Request can be seen in Annex 6.

18 Disclosure of personal information

All staff and volunteers, including the Trustees, should be familiar with the Confidentiality Policy, which set out Talking Money'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; First line of address & Postcode.
- If individuals or other agencies contact Talking Money 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 Talking Money.
- 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 Talking Money client.
- If the enquirer has correspondence from Talking Money, 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 on the P drive, which only the Leadership Team and Finance Officer can access. These details must not be given to anyone outside Talking Money 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 colleagues and/or the Chief Executive. 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.

Data held in personnel files/ HR Database

The following data is held in personnel files:

- CV
- Induction – to include: Bank account details, Next of Kin
- References
- Correspondence – Resignation
- Contract - Copy of contract of employment, Confirmation of job offer, Evidence of
- right to work in the UK
- Training
- Job description
- Supervision notes/Appraisal notes

No additional information will be kept as a matter of routine but other documents may be kept for specific reasons e.g:

- Arrangements relating to periods of leave – paid or unpaid
- Requests for information e.g. for mortgages, rental agreements
- Warnings under the disciplinary procedure
- 'Right to be forgotten' means that if you no longer want your data to be processed and provided that there are no legitimate grounds for retaining it, the data will be deleted; Otherwise it is automatically destroyed after being held on file for six years.

19 Access

The personnel files are held in the locked filing cabinet in the Admin office. Workers are entitled to access their own files with permission from their Manager. Nobody is entitled to access another worker's file without the worker's explicit consent, other than the line manager, Chief Executive or the manager who is responsible for maintaining the personnel files, information is also stored within the HR Database held on the P Drive.

20 Personal information record

New workers are asked to complete a Personal Information Sheet which is kept with the personnel files and is used only in case of emergency. This information is also held electronically within the HR database. The personal information sheet has details of who to contact in an emergency and details of any medical information that first aiders or medical attendants may need in a situation where the worker cannot give the information her/himself.

21 Personnel file destruction

Talking Money will follow the Information Commissioner's Code of Practice on employment records.

Personnel files are destroyed securely six years after the worker leaves Talking Money. Prior to this they are stored separately in a locked filing cabinet, which only the Chief Executive and managers have access to, with the date for destruction marked on them.

22 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.

23 Data Breaches

Any breach of this policy or of data protection laws must be reported within 72 hours. Talking Money has a legal obligation to report any data breaches to Information Commissioner's Office.

If there is a high risk to the rights and freedoms of individuals, data subjects 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 either in their own right or as part of a pattern of failures

For a full data breach checklist see Annex 7.

24 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 Talking Money is registered with the Information Commissioner's Office with the number Z4759465.

Annex 1 - DEFINITIONS

Data Controller - A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Processors - A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Special Categories of Data - "Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

Process, Processed, Processing - Any operation or set of operations performed on

Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection - The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Consent - Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Supervisory authority - This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office

Annex 2 – LEGAL BASES FOR PROCESSING

1. We may process personal data that are provided in the course of the use of our services. The service data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with persons or entities. The legal basis for this processing is consent and/or our legitimate interests, namely the proper administration of the charity and/or the performance of a contract between them and Talking Money and/or taking steps, at their request, to enter into such a contract.

2. We may process data contained in or relating to any communication that persons or entities have with us. The correspondence data may include the communication content and metadata associated with the communication. The correspondence data may be processed for the purposes of communicating with them and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of the charity and our communications with users.

3. We may process any of your personal data identified in this policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

4. We may process any of your personal data identified in this policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

5. In addition to the specific purposes for which we may process your personal data set out in this Section 3, we may also process any of your personal data where such processing is necessary for

compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

Providing your personal data to others

1. We may disclose your personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.
2. We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
3. Financial transactions relating to our website and services may be handled by our payment services providers. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds.
4. We may disclose personal data funders, research organization or auditors for the purpose of evaluating our services, creating statistics performance reports or evaluations and carrying out reviews audits or inspections. Each such third party will act as a data controller in relation to the enquiry data that we supply to it; and if contacting you, each such third party will supply to you a copy of its own privacy policy, which will govern that third party's use of your personal data.
5. In addition to the specific disclosures of personal data set out in so far, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

Annex 3 – PRIVACY NOTICE

Introduction

Talking Money is committed to protecting your privacy and security. This notice explains how and why we use your personal data, to ensure you remain informed and in control of your information. (RSPB)

Questions?

Any questions you have in relation to this privacy notice or how we use your personal data should be sent to mail@talkingmoney.org.uk or addressed to The Data Officer, Talking Money, 1 Hide Market, West Street, St Philips, Bristol BS2 0BH

What is personal data?

Personal data is information that can be used to help identify an individual, such as name, address, phone number or email address.

The policy in brief

Here is a brief summary:

- We collect personal data (as outlined above) to be able to work on behalf of our clients, helping them with their money worries, to fundraise for our work and for administration, research and analysis
- We do our very best to keep personal information safe and secure
- We only share data where we are required by law or with carefully selected partners who do work for us or fund the work that we do. We never sell your data and we will never share it with another company or charity for marketing purposes.
- We will only retain your data for as long as it is required.
- These are the basics, but you can read the full policy (below).

What information we collect and why?

- It is your choice what information you share with us, however if you do choose to withhold requested information, we may not be able to provide you with certain services.
- We will only collect personal information where this is strictly necessary for legitimate organisational purposes;

- We collect only the minimum personal information required for these purposes
- We may also need to share your data with other organisations or partner agencies in order to advance your case.
- If you give us permission for us to share your details with our funders for satisfaction monitoring purposes, they, or an agency appointed by them, might contact you by phone.
- If you give us permission to share your details and case file with our funders for quality monitoring, your issue and the advice you received may be reviewed and feedback given to your adviser (CA)
- Research and surveys - in order to continually improve the services we provide, we may contact you directly or through selected research companies in order to conduct voluntary surveys, recording and analysing this information to improve the quality and effectiveness of what we do
- Management reporting and planning - we produce internal documents in order to monitor our own activities

Keeping your information safe and secure

We place a great importance on the security of all personally identifiable information associated with our supporters, clients and staff. We have security measures in place to protect against the loss, misuse and alteration of personal data under our control. (SSAFA)

Sharing your information

We will only share your information with your consent and only with those that have signed a contract that requires them to:

- Abide by the requirements of the General Data Protection Regulation
- Treat your information as carefully as we would
- Only use the information for the purposes it was supplied (and not for their own purposes or the purposes of any other organisation)
- Allow us to carry out checks to ensure they are doing all these things.

Disclosures required by law - the law can require the disclosure of information for various reasons, in such circumstances Talking Money must comply with those requests

How we'll store your information – Clients

We'll store the record of your case in a secure case management system, which is only accessed by us. Paper copies of your information may also be stored securely and accessed by staff and volunteers of Talking Money.

How we'll store your information - Staff

When you apply for a job with Talking Money, your personal data will be collated in order to monitor the progression of your application. Where we need to share your data – such as gathering references, obtaining a Disclosure and Barring Services/Disclosure Scotland check (depends on the role) or a prison clearance (depends on the role) – you will be informed beforehand, unless the disclosure is required by law. These checks are only done after a position has been offered only to the successful candidate. On the application form, you are asked to complete the referee details and can tick permission to contact referee. If tick yes, once offered a role, we will automatically send out reference requests. If tick no, we will contact successful candidate for permission first.

Personal data about unsuccessful applicants are held for 12 months after the recruitment exercise is complete for that particular vacancy. Applicants can ask us to remove your data before this time if you do not want us to hold it. If we feel there is another suitable vacancy available, we will contact the applicant prior to sharing your application details with the relevant manager.

Once you have taken up employment with Talking Money, we will compile a file relating to your employment. The information contained in this will be kept secure and will only be used for purposes directly relevant to your employment. Once your employment with Talking Money has ended, we will retain the file for six years and then delete it from our files unless you request for it to be deleted before this time. (Shelter)

Access to your information and correction

You have the right to make a Subject Access Request to ask for a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please email or write to us at the following, specifying that you are making a Subject Access Request: mail@talkingmoney.org.uk or addressed to The Data Officer, Talking Money, 1 Hide Market, West Street, St Philips, Bristol BS2 0BH.

We want to make sure that your personal information is accurate and up to date. You may ask us to correct or remove information you think is inaccurate.

Your rights

The Data Protection Act gives you certain rights over your data and how we use it. These include:

- a right of access to a copy of the information comprised in your personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;

- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

To find out more about what these rights mean for you, refer to the Information Commissioner's website: https://ico.org.uk/ (CABA)

Other websites

Our website contains links to other websites. This privacy policy only applies to this website so when you link to other websites you should read their own privacy policies.

Changes to our privacy policy

We keep our privacy policy under regular review and we will place any updates on this web page. This privacy policy was last updated on 16 May 2018.

Annex 4 – THE RIGHTS OF INDIVIDUALS

Right of the individual under data protection law are:

1. the right to access;
2. the right to rectification;
3. the right to erasure;
4. the right to restrict processing;
5. the right to object to processing;

6. the right to data portability;
7. the right to complain to a supervisory authority; and
8. the right to withdraw consent.

1. You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.
2. You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.
3. In some circumstances, you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.
4. In some circumstances, you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.
5. You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims. You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose. You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical

purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

6. To the extent that the legal basis for our processing of your personal data is:
    a. consent; or
    b. that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.
7. If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with the Information Commissioner's Office. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.
8. To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

You may exercise any of your rights in relation to your personal data by written notice to us.

Annex 5 - CONSENT

Data Protection Statement

Client data Protection declaration

Due to our funding requirements and as part of our Advice Quality Standard accreditation we need to provide information about our clients to funders and auditors.

The information you give may be

1) added to a secure and confidential database

2) passed to a research organisation to evaluate our projects

3) used by our funders or their agents to create st atistics, performance reports or evaluations

4) accessed by our auditors to carry out reviews, audits or inspections

We may also need to share your data with other organisations or partner agencies in order to advance your case and, where necessary, to protect public funds or if we are lawfully required to do so. If you do not want your personal information used in this way, we may not be able to offer some of our services to you.

Any information provided will be treated confidentially and in accordance with the Data Protection Act 1998. You have the right to make formal request in writing for access to persona l data held about you, to inspect it, and to have it corrected if it is wrong. We keep the information you supply to us and any work we carry out on your behalf in electronic format for 6 years, after which time it will be securely destroyed. Your information will never be sold to external parties.

Talking Money' s full Data Protection Policy is available upon request.

By signing this document, I confirm that I understand and agree for my personal information to be used as described:

Client Signature Date:

Annex 6 – SUBJECT ACCESS REQUESTS (SAR)

Step 1. A SAR must be identified. The request must be made in writing unless the person has a disability meaning they are unable to do so, then another reasonable means can be agreed. The person does not need to mention the specific act or use the term “Subject Access Request” for it to be a valid request so it is important to that staff can recognise a SAR and treat it appropriately.

Step 2. The request must be validated with proof of photo ID or proof of address.

Step 3. When handling request made by third parties or children. The third party making the request must provide evidence that they are entitled to act on behalf of the individual. A child must be able to understand their rights and understand (in broad terms) what it means to make a SAR how to interpret the information they receive as a result of doing so.

Step 4. Remove any irrelevant third party data or data that you are legally exempt from disclosing.

Step 5. Provide an individual with a copy of the information the requested, free of charge. This must occur without delay, and within one month of receipt. Talking Money endeavour to provide data subjects access to their information in commonly used electronic formats

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

Talking Money can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual to specify the information they are requesting.

Once a SAR has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Step 6 Maintain a record of any action taken towards conducting or completing a SAR

Annex 7 – CHECKLIST FOR DATA BREACHES

1. Mobilise the Leadership team
2. Assess level of risk of data breach – no risk/risk/high risk – if unaddressed such a breach is likely to have a significant detrimental effect on individuals /data subjects
3. Inform the ICO within 72 hours
4. Leadership team to keep records of response to the data breach
5. Identify key internal and external messaging for communications strategy and issue
6. Secure IT systems
7. Stop additional data loss
8. Speak to those affected/involved: If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.
9. Identify key issues and extent of data breach
10. Review protocols about disseminating information about the breach for everyone involved
11. Begin an in-depth investigation, using forensics if necessary
12. Report to police when/if considered appropriate
13. Notify regulators/consult with legal team/insurers

What information must a breach notification contain?

1. The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned;
2. A description of the likely consequences of the personal data breach; and
3. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.