OB08: Data Protection Policy & Procedures

1. Introduction and policy statement

1.1. After Adoption is committed to a policy of protecting the rights and privacy of individuals (including employees, students, volunteers, service users and others) in accordance with the Data Protection Act 1998, as amended. After Adoption fully endorses and adheres to the eight principles of the Data Protection Act (see Section 5 below). These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, and processing, transporting and storing personal data. Employees and others who obtain, handle, process, transport and store personal data for After Adoption must adhere to these principles.

1.2. After Adoption needs to process certain information about its staff, service users and other individuals it has dealings with for various purposes, including:

- Furthering the information, advice, support and training provided to service users of the organisation.
- For administrative purposes (eg, recruiting, employing, supporting and paying staff, including volunteers and students) (including current, past and prospective employees).
- For the purposes of fundraising, managing conferences, seminars, training
- For the purposes of securing and maintaining services from external suppliers.

1.3. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

1.4. This policy applies to all After Adoption employees (including self employed), students and volunteers (including trustees). Any breach of the Data Protection Act or After Adoption's Data Protection Policy will be subject to After Adoption's disciplinary procedures (PM EM04)

2. Purpose of the Data Protection Act

2.1. The purpose of the Act is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge and, wherever possible, is processed with their consent.

2.2. The main aims of the Act are to :

- require data users to be open about the collection and disclosure of personal data and to ensure adherence to a series of principles that are designed to prevent the misuse of data
- guard everybody from any harm or distress which could be caused by information getting into the wrong hands and
- accord to individuals a number of rights in respect of access to, information about and prohibition in the processing of data.

3. Definitions from the Act

3.1. *Personal data*

Means data which relate to a living individual who can be identified from those data, or from data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.2. *Sensitive data*

Different from ordinary personal data (such as name, address, telephone number) and relates to racial or ethnic origin, political opinion, religious or other beliefs of a similar nature, physical or mental health, sexuality, the commission or alleged commission of any offence, criminal convictions, or family circumstances. Sensitive data is subject to much stricter conditions of processing.

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

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

3.5. *Processing*
Any operation related to the organisation, retrieval, disclosure and deletion of data and includes: obtaining and recording data; accessing, altering, adding to, merging, and deleting data; retrieving, consulting on or using data; disclosing or otherwise making available data.

3.6. *Third party*
Any individual or organisation other than the data subject, the data controller (i.e. After Adoption) or its agents.

3.7. *Relevant filing system*
Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Note that this is the definition of "relevant filing system" in the Act. Personal data, as defined and covered by the Act, can be held in any format, such as electronic (including websites and emails), paper-based, photographic, etc, from which the individual's information can be readily extracted.

3.8. *Fairly*
Means that the data subject has been provided with, or had the following information made available to them: the identity of the data controller, the purposes for which the data is to be processed and any further information which is necessary in the circumstances to allow the processing to be fair.

3.9. *Fairness Information*
Is the information that must be provided to the data subject in order to ensure that the processing is fair.

4. Responsibilities under the Data Protection Act

4.1. The responsibility for implementation of this policy rests with the Chief Executive, the Senior Management Group and the Data Protection Officer.

4.2. After Adoption will ensure that:

- Everyone managing and/or handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and/or handling personal information is appropriately trained to do so.
- Everyone managing and/or handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information whether a member of staff or a member of the public, is given advice as necessary.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated

- Employees are aware of the action required in the event of Data Breach

4.3. On joining After Adoption, employees are required to undertake training on Data Protection as part of their induction.

4.4. The Data Protection Officer will work with the management group to raise awareness and maintain a high level of understanding of Data Protection among key staff and to communicate any legal or policy changes that occur.

4.5. Supporting procedures for this policy may be created as and when they are required and will be subject to an appropriate level of consultation before implementation.

4.6. Data protection audits will be carried out by internal audits in order to monitor compliance with the DPA and this policy.

5. Responsibilities under the Data Protection Act

5.1. After Adoption has the following responsibilities:

- The Director of Finance and Support Services has been appointed as Data Protection Officer and is responsible for the day-to-day data protection matters and for developing specific procedures and practices on data protection issues for After Adoption.
- Compliance with data protection legislation is the responsibility of all After Adoption staff who process personal information.
- Service users and others who supply personal data to After Adoption are responsible for ensuring that any data supplied is accurate and up-to-date.

6. Data protection principles

6.1. The Act's principles require that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for specific and lawful purposes and shall not be processed in any manner incompatible with those purposes.
- Be adequate, relevant and not excessive for those purposes – information that is not strictly necessary for the purpose for which it is obtained should not be collected. If data is given or obtained that is excessive for the purpose, then it should be immediately deleted or destroyed.
- Be accurate and, where necessary, kept up to date – data, which are kept for a long time, should be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume they are accurate. It is the responsibility of individuals to ensure that data held by After Adoption is accurate and up to date.
- Not be kept for longer than is necessary for that purpose – see section 12 on retention and disposal of data.
- Be processed in accordance with the data subject's rights – see section 6 on rights.
- Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using appropriate technical and organisational measures – see section 8 on security.
- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data – staff should be aware of this when publishing information on the organisation's' website, which can be accessed from anywhere in the world (data transfer includes placing data on a website that can be accessed from outside the EEA (ie, European Union member states, but including Liechtenstein and Iceland)).

7. Data subject rights

7.1. Data subjects have the following rights regarding data processing, and that data that is recorded about them:
- To make subject access requests regarding the nature of the information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of any automated decision-taking processes that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated processes.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Information Commissioner to assess whether any provision of the Act has been contravened.

7.2. Further details of service user access to records held about them are included in the Access to Information Policy (AS02).

8. Consent

8.1. Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed, unless the individual has given consent. After Adoption understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for proceedings exists.

8.2. In most instances, consent to process personal and sensitive data is obtained routinely by After Adoption (e.g. through a prospective adopter, adoptive parent or other service user completing a consent form, see Recording Policy AA04, at the initial point of contact in person or on the telephone or a new member of staff signing a contract of employment).

8.3. Any After Adoption form (whether paper-based, electronic or web-based) that gathers data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on After Adoption's website, as such data can be accessed from all over the world.

8.4. If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that processing does not take place.

9. Security of data

9.1. All staff are responsible for ensuring that any personal data (on other individuals) which they hold is kept securely and that it is not disclosed to any unauthorised third party.

9.2. All personal data should be accessible only to those who need to use it.

9.3. In relation to security of data, staff should form a judgement based upon the sensitivity and value of the information in question, but personal data should always be kept:
- In a lockable room with controlled access; or
- In a locked drawer or filing cabinet; or
- If computerised, password protected, or
- Kept on disks, tapes or other IT memory storage devices, which are themselves kept securely.

9.4. Care should be taken to ensure that computers and terminals are not visible except to authorised staff and that computer passwords are kept confidential. Computer screens should not be left unattended without password-protected screen-savers and manual records should not be left where they can be accessed by unauthorised staff.

9.5. After Adoption ensures that service user information or case records are kept in locked filing cabinets, where it is held in a paper-based form. In the case of electronic information, this is stored on individual personal computers (PCs) and on After Adoption's central server, with access to folders controlled by different levels of permissions, with access to those folders only provided to staff who need to see the information. Individual computers are password-protected. A daily back-up of After Adoption's centrally-held electronic information including the organisational database is carried out. The back-up is stored securely with month-end back-ups being stored securely off-site.

9.6. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Personal shredders are available for After Adoption staff (whether home of office-based).

9.7. Hard drives of redundant computers should be removed or wiped clean before disposal – the Director of Finance arranges for this to be done.

9.8. This policy also applies to staff (eg, home workers and volunteers) who process personal data away from After Adoption offices. Such processing away from After Adoption's offices presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing data at home or in locations away from After Adoption offices.

9.9. The Home Working Policy (HS13) also includes reference to the secure storage of all After Adoption files. Staff should not carry out After Adoption work on their home computers.

10. Transport of electronic & printed data

10.1. Avoid taking hard copy information containing personal data away from After Adoption offices to contract management or other meetings. This includes documents, files and printed emails. Wherever possible we will work together to utilise technology available to us, such as encrypted e-mails to avoid the need to produce hard copies. This should also reduce the costs associated with printing and distribution of materials for us.

10.2. Where necessary, local authority staff can print information on our behalf and disseminate it within the meeting. This can be achieved by sending the information electronically to local authorities using a secure email service in advance of any planned meetings (see below). By adopting this approach the risk of information being lost on route to the meeting is removed.

10.3. If transporting hard copy information is completely unavoidable then the following controls should be implemented:

- Use anonymised information where possible.
- Print off only the minimum necessary to achieve your aim.
- Transport in a locked briefcase or bag with the Helplines telephone number on the outside
- Ensure the locked briefcase/bag remains in your custody at all times.
- Ensure paper records are securely destroyed when no longer required e.g. cross cut shredder.
- Extreme vigilance

11. Email Security

11.1. **Standard email is not secure and therefore must never be used for the transmission of personal and sensitive information about service users or staff**.

11.2. After Adoption has email encryption available. This is the simple use of the tagline "#encrypt" at the start of the subject line, or click on the 'Encrypt Email' button on the ribbon of your Outlook programme. This will ensure that the e-mail and any attachments are fully encrypted as the e-mail leaves the After Adoption mail server – you will receive confirmation that the e-mail has been sent to the recipient(s) in encrypted format. You will have to provide the e-mail recipient with the password (via telephone conversation) in order for them to open both the e-mail and its attachments. Note, that internal emails will NOT be encrypted as they never leave the secure server environment.

11.3. When you start to type in the name of the recipient, the email software may suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way – eg. "Dave" – the auto complete function may bring up several "Daves". **Make sure you choose the correct address before you click send.**

11.4. If you want to send an email to a recipient without revealing their address to other recipients, use the blind carbon copy (bcc) function, not carbon copy (cc). When you use cc every recipient of the message will be able to see the addresses it was sent to. The benefits for using the bcc function include:

- **Privacy** - Sometimes it's beneficial, even necessary, for you to let recipients know who else is receiving your email message. However, there may be instances when you want to send the same message to multiple recipients without letting them know who else is receiving the message. If you are sending email on behalf of a business or organization, it may be especially important to keep lists of clients, members, or associates confidential. You may also want to avoid listing an internal email address on a message being sent to external recipients. Another point to remember is that if any of the recipients use the "reply to all" feature to reply to your messages, all of the recipients listed in the **To:** and **CC:** fields will receive the reply. If there is potential for a response that is not appropriate for all recipients, consider using BCC.
- **Tracking** - Maybe you want to access or archive the email message you are sending at another email account. Or maybe you want to make someone, such as a manager or team member, aware of the email without actually involving them in the exchange. BCC allows you to accomplish these goals without advertising that you are doing it.
- **Respect for your recipients** - People often forward email messages without removing the addresses of previous recipients. As a result, messages that are repeatedly sent to many recipients may contain long lists of email addresses. Spammers and email-borne viruses may collect and target those addresses. To reduce the risk, encourage people who forward messages to you to use BCC so that your email address is less likely to appear in other people's inboxes and be susceptible to being harvested. To avoid becoming part of the problem, in addition to using BCC if you forward messages, take time to remove all existing email addresses within the message. The additional benefit is that the people you're sending the message to will appreciate not having to scroll through large sections of irrelevant information to get to the actual message.

11.5. Take care when using group email addresses. Check who is in the group and make sure you really want to send your message to everyone.

11.6. If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

11.7. In some cases, Local Authorities have their own e-mail encryption systems, which you may be able to join at their invitation. This is achieved by replying to a secure email sent by the LA to you. Instructions are normally attached to assist you with the process.

12. Disclosure of data

12.1. After Adoption must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and, in certain circumstances, the police. All After Adoption staff should exercise caution when asked to disclose personal data held on another individual to a third party. Where this is a service user, the presumption should be not to disclose information to another unless one of the conditions below applies.

12.2. Under this policy, personal data may legitimately be disclosed where one of the following conditions apply:

- The individual has given their consent
- Where disclosure is in the legitimate interests of After Adoption (e.g. disclosure of personal information to staff so that they can carry out their work in providing support to service users).
- Where After Adoption is legally obliged to disclose the data (e.g. through OFSTED or Charity Commission inspections or inquiries, police investigations, by order of court, etc).
- Where disclosure of data is required for the performance of a contract.
- Where After Adoption becomes aware of a child or vulnerable adult Safeguarding concern or identifies a potential risk to another service user or another person and decides to inform the relevant authorities

12.3. As one example, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work-related matter. It is important to consider whether or not disclosure of the information is relevant to, and necessary for, the conduct of After Adoption's work. Best practice would be to take the contact details of the person making the enquiry and pass them onto the colleague concerned.

12.4. Similarly, if staff members receive enquiries as to whether or not a named individual is an After Adoption service user, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the staff member should decline to comment. Even confirming whether or not an individual is an After Adoption service user may constitute an unauthorised disclosure and would be a breach of After Adoption's Confidentiality Policy (OB04).

12.5. Unless consent has been obtained from the data subject (e.g. service user), information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally, a statement from the data subject consenting to disclosure to the third party should accompany the request.

12.6. As an alternative to disclosing personal data, After Adoption may offer to do one of the following:

- Pass on a message to the data subject asking them to contact the enquirer.
- Accept an incoming email message and attempt to forward it to the data subject. After Adoption will not accept sealed envelopes or packets for forwarding to members or service users. Due to the many sensitivities of adoption, After Adoption does not want to be responsible for forwarding unknown messages or materials to its service users or adoptive parents and prospective parents.

13. Rights of access to data

13.1. Service users and staff of After Adoption have the right to access any personal data which is held by the organisation in electronic format and manual records which form part of a relevant filing system.

13.2. Anyone who wishes to exercise this right should apply in writing to the Data Protection Officer (see contact details below). After Adoption reserves the right to charge a fee (currently £10) for data subject access requests. Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

14. Use of data

14.1. To further the information, advice, support and training that be can provided to service users, the personal information collected is used for the following purposes:

- To post/circulate our fundraising and general communications and other organisational information.
- To keep our accounts up to date.
- To identify service users when they contact the Helpline or other support services.
- To compile non-identifying statistical information on the composition of the service users and services provided.

14.2. In relation to personal information held by After Adoption on employees, volunteers, students and trustees, see Appendix 1.

15. Retention and disposal of data

15.1. After Adoption discourages the retention of personal data for longer than they are required. Considerable amounts of data can be collected on individual members and staff. However, once a member has let their membership lapse or once a staff member leaves the organisation, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

However, After Adoption is under a statutory duty to retain all data and documentation relating to cases of adoption and the provision of adoption support services for a period of 100 years.

15.2. *Staff*

15.2.1. In general, staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. More detailed information held on the employment file (eg, records relating to the staff member's work for After Adoption) will be kept for six years from the end of employment. Information relating to income tax, Statutory Maternity, Paternity and Adoption Pay, etc, will be retained for the statutory time period of six years for financial and tax records.

15.2.2. Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date.

15.2.3. See Appendix 1 for further information in relation to data protection issues for employees, students, volunteers and trustees. See OB09a for details referring to the retention of the Staff Records.

15.3. *Disposal of records*

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

16. Publication of After Adoption information

16.1. All staff should note that After Adoption publishes a number of items that include personal data, and will continue to do so. These personal data are:

- Information published in various publications including names, job titles and work contact details of members of staff (and sometimes photos of some staff).

- Information published on After Adoption's website, including names, job titles and work contact details of some members of staff.
- Information in promotional material, annual reports (sometimes including photos of some staff), staff newsletters, etc.

16.2. It is acknowledged there may be occasions when a staff member requests that their personal details in some of these categories remain confidential or are restricted to internal access. Where possible and practicable, After Adoption will comply with the request and ensure that appropriate action is taken. However, where the information is published with the aim of meeting service users' needs for support services (e.g. name, job title and work contact number published in order to promote the availability of a specific service), there may be a limit to what further action After Adoption can take.

17. Direct marketing

17.1. Any team or department that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

18. Monitoring

18.1. Every manager is responsible for monitoring and acting upon any Data Protection breaches and near misses using the framework of this policy when an issue arises within their team.

18.2. Every member of staff is responsible for notifying their manager of any breach or near miss.

18.3. Failure by any member of staff to adhere to this policy may result in disciplinary action.

18.4. The Director of Finance & Support Services is responsible for the monitoring, reviewing and updating of this policy on a 3 yearly basis or sooner if the need arises.

18.5. Compliance with the policies and procedures as set out in this document is monitored on a monthly basis by the Director for Finance & Support Services and the Quality Standards Manager, together with independent review by the Senior Management Group.

18.6. Lessons learned will also be discussed following any near miss or actual breach, thereby reducing the likelihood of a similar incidence and promote good working practice.

19. Monetary Penalties/Fines

19.1. The Information Commissioner has the power to fine organisations (and individuals) for serious breaches of the Data Protection Act. This is also called the power to issue a Monetary Penalty Notice. The Commissioner can require payment of a sum up to £500,000. Fines have been made against organisations that faxed sensitive personal data to the wrong recipients, lost a laptop that held personal data because of a burglary and lost unencrypted laptops that held personal data. All fines are made public by the Commissioner and the Chief Executive of the offending organisation is usually asked to make a formal undertaking to put in place effective measures and remedies.

20. Reporting Breaches/Timescales

20.1. All data protection breaches and near misses must be reported and submitted to the Director of Finance & Support Services using the incident report form OB08a. A copy must also be sent to the Deputy Chief Executive and Quality Standards Manager.

21. Data Protection Officer

21.1. After Adoption's Data Protection Officer is:
Donald Lowe

Director of Finance
After Adoption, Unit 5 Citygate, 5 Blantyre Street, Manchester, M15 4JJ

21.2. In the absence of the above, please contact either:
Lynn Charlton
Chief Executive
After Adoption, Unit 5 Citygate, 5 Blantyre Street, Manchester, M15 4JJ

21.3. or
Tracey Beekman
Business Development Manager
After Adoption, Unit 5 Citygate, 5 Blantyre Street, Manchester, M15 4JJ

22. Other related legislation

There is significant legislation across the public sector in relation to data and information governance, including:

- EC Data Protection Directive
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Computer Misuse Act 1990
- Privacy & Electronic Communications Regulations 2003
- Children Act 2004

23. References

AA04 – Recording Policy
AS02 – Access to Information Policy
HS13 – Home Working Policy
OB04 – Confidentiality Policy
OB08a – Incident Reporting form
PM EM04 – Disciplinary Policy

APPENDIX 1
Data protection policy in relation to After Adoption information on employees, volunteers, students and trustees

1. Introduction

1.1. This appendix outlines After Adoption's data protection policy and procedures specifically in relation to employees, workers, volunteers, students and trustees. It sets out what After Adoption will do with employees', volunteers', students' and trustees' information, and defines individuals' rights of access to their information and their responsibilities in relation to data protection.

2. Policy

2.1 All staff (employees, workers, volunteers, students and trustees) are covered by the Act. Visitors who are given access to computers, manual records or other media may also be covered. They are therefore required to understand the rights and responsibilities with regard to data, which they are using or processing. The Act covers all documents, which are structured by reference to individuals so that specific information is readily accessible, i.e. kept on a relevant filing system.

2.2 The legislation covers computer files and manual files which includes paper, microfiche or any other material which can be printed on. In other words all information held on desktop PCs, laptops and notebooks including any work stored at home, either manually or electronically.

2.3 In relation to general data protection issues, After Adoption has a Data Protection Officer (DPO) (currently the Director of Finance) to ensure that we meet the requirements of the Act. The DPO is responsible for our notification as a data user under the Act, and any queries in relation to data protection should be referred to the DPO. The Chief Executive and Trustees oversee compliance.

3. The Data Protection Act 1998

3.1 The Act outlines eight data protection principles. In relation to staff information, After Adoption addresses these as follows.

- Personal data shall be processed fairly and lawfully

3.2 In practice what this means for the processing of information is that the After Adoption can, subject to certain limitations, process personal information in the normal course of administration. Examples of typical uses of staff information are:

- Recruitment.
- Administration and payment of wages, salaries, pensions and other benefits.
- Negotiation or communication with employees.
- Employee assessment and training, human resources and career planning.
- Compliance with policy and/or legislation with regard to health, safety or other employment matters.
- Job or task scheduling or roster administration.
- Identification of resources.
- Monitoring the use of equipment or services.
- Analysis for management purposes and statutory returns.
- Provision of references.
- Training and development.

3.3 Sensitive data will only be held and processed in one of the following circumstances:

- If the data subject has given his/her explicit consent.
- For the purpose of monitoring equality of opportunity.

- In order to exercise a right or obligation conferred or imposed by law, such as revealing information about past convictions in order to protect children under the Children Act.
- In connection with legal proceedings or to obtain legal advice.
- For the exercise of the functions of a Government department, such as tax returns to the Inland Revenue and national insurance payments to the Contributions Agency or statistical returns to funding agencies.
- To protect the individual's interests where it is not possible to obtain the individual's consent, or After Adoption cannot reasonably have been expected to obtain the individual's consent.
- The individual has deliberately made the data public, for example, by talking to the media or writing an article.
- For medical purposes such as an examination carried out or a report written by a health professional.

3.4 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any matter incompatible with that purpose or those purposes.

3.5 After Adoption undertakes to obtain data fairly, and the data subject will be told who the data controller is and what the data will be used for.

3.6 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.7 After Adoption undertakes to restrict requests for information to those areas which are strictly necessary for the performance of a contract of employment and to the functioning of After Adoption as a Voluntary Adoption Agency and Adoption Support Agency. After Adoption will review personal files and other information to ensure that they do not contain information, which is excessive, and will destroy any such information. Destruction of data will be in accordance with earlier sections of this policy.

3.8 Personal data shall be accurate and, where necessary, be kept up to date.

3.9 After Adoption undertakes to maintain its files accurately and to ensure the information contained is up-to-date and to carry out regular audits on the accuracy of data.

3.10 All staff should also ensure that After Adoption has the most accurate, up-to-date personal information on record, and should notify the Human Resources Manager or Director of Finance of any changes, e.g. to their address, telephone numbers, qualifications, etc.

3.11 Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

3.12 After Adoption will keep under review the length of time that information is held, and the purposes for which it is held. Where there is no legal requirement to retain personal data, After Adoption reserves the right to de-personalise the data to prevent identification of particular individuals for historic, statistical or research purposes.

3.13 See separate policy for the Document Retention Schedule (OB09a).

3.14 Personal data shall be processed in accordance with the rights of data subjects.

3.15 After Adoption will keep individuals informed about whether any data relating to an individual is being processed, what the data consists of, the purposes for which the data is being processed, and the recipient of the information. Employees will be informed about the logic in decision-making where processing by automatic means is the sole basis for any decision significantly affecting them; After Adoption undertakes not to make decisions about recruitment, appraisal and promotion exclusively on the basis of automatic means such as computer software.

3.16 The appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

3.17 After Adoption undertakes to ensure security in respect of data, to ensure no unauthorised access either physically into the office premises or manual filing systems, or into the computer hardware or software.

3.18 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.19 After Adoption will not transfer any data without satisfying the standards required under the Act, which does place restrictions on where data may be sent. This will include data published on its website.

4.0 Security of data

4.1 To ensure that security is maintained in relation to the information that After Adoption holds, all staff must observe the following provisions:

- Access to personal data on staff held on office computers, personal and laptop computers, compact disks or other electronic media and manual files must not be allowed to any person without the express permission of the Chief Executive or Human Resources Manager.
- Personal data relating to staff, workers, volunteers, students and trustees must not be entered into, amended or deleted from any computer, personal or laptop computer, microfiche, compact disk, floppy disk or manual file without the express prior authorisation or permission of the Chief Executive or Human Resources Manager or in accordance with written procedures or instructions issued by him/her.
- Disclosure of any personal data held in any form must not be made to any person without the express prior permission of the Chief Executive or Human Resources Manager or in accordance with written procedures or instructions issued by him/her.
- Members of staff must not seek to obtain by any means any personal data held by or on behalf of After Adoption in any form, except on a genuine 'need to know' basis or arising directly from their own duties and responsibilities.

4.2 Members of staff should be aware that under the Act they are personally accountable for their actions and can be held criminally liable if they knowingly, recklessly or fail to observe or breach these rules. Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under After Adoption's Disciplinary Procedure. If an employee accesses another employee or worker's personnel records without authority this constitutes a gross misconduct offence and could lead to summary dismissal.

5.0 The role of the Data Protection Officer (DPO)

5.1 Non-compliance with the Data Protection Act can be a criminal offence, and can result in sanctions including unlimited fines, for example, for using personal data for a purpose other than described in the entry in the Data Protection Register. More typically, a fine of £5,000 can be imposed for offences such as supplying false or misleading information to the Information Commissioner. The DPO has been appointed to ensure that:

- all data is processed fairly.
- the data is accurate, and that processes exist to check and amend data as necessary.
- consent from data subjects is obtained either generally or expressly.
- data is kept securely and disposed of properly.
- notification requirements are satisfied.
- determinations are made regarding the processing of data without consent in cases of necessity or public interest.

6.0 The role of the employee

6.1 Every employee must comply with this policy. Failure to comply with the policey may result in disciplinary action which could include dismissal.

6.2 It is a criminal offence to access personal data held by After Adoption for other than After Adoption business, or to procure the disclosure of personal data to a third party.

6.3 Although the Trustees of After Adoption are the registered data controller, employees can be designated as data controllers to deal with day-to-day matters. The Act places a personal liability on any manager, administrator or similar officer (or any person purporting to act in such capacity) in the event of any offence being committed with his/her consent or connivance or attributable to his/her neglect; i.e. the individual may be liable to prosecution as well as After Adoption.

6.4 All employees should therefore ensure that they abide by the principles of the Data Protection Act and this Policy. In particular they must not collect, process or disclose any data without checking whether:

a) After Adoption is registered to do so, and
b) It is in a manner which complies with the Act. Any queries must be referred to the Chief Executive or Director of Finance.

7.0 Access to information

7.1 The Chief Executive or Human Resources Manager will provide, as appropriate, a printout of the information contained in the computerised personnel system for individuals to check and amend as necessary.

7.2 Only the Chief Executive, Director of Finance, Deputy Chief Executive, Human Resources staff and Finance will have access to personal information, and After Adoption undertakes to carry regular audits of the files that it holds, to ensure that:

- it does not hold any data or information which is out-of-date or irrelevant
- sensitive data is excluded from files except with the express permission of the data subject
- it destroys all papers of those members of staff who have not worked for After Adoption for more than six years.
- data is only used for the purposes for which it is intended

7.3 Specific employee information will be held as follows:

- ***Facts of employment*** - Information on staff appointment and leaving dates, and the job/roles carried out, will be held by After Adoption in perpetuity – for the purposes of being able to supply references and confirm employment or voluntary work
- ***Appraisal records*** - After Adoption undertakes to keep appraisal reports for a maximum of fifteen years after termination of employment, after which they will be destroyed.
- ***Employment Applications*** - Paperwork relating to employment applications will be held for fifteen years after termination of employment, after which it will be destroyed.
- ***References*** - References issued for external posts will be prepared and issued on a confidential basis. References received for new employees will be held for fifteen years after termination of employment, after which they will be destroyed. References issued should be prepared and issued on a 'private & confidential' basis.

8.0 Recruitment papers and associated electronic communications

8.1 All papers and items of electronic communication relating to unsuccessful applicants will be destroyed six months after a successful appointment is made.

9.0 Rights of data subject

9.1 Section 6 of this policy sets out the rights of data subjects.

9.2 Current or past employees, workers, volunteers, students or trustees can exercise the right of access to personal files by making a written request to the Chief Executive or Director of Finance for a copy, or original if this is not possible, of a file which makes reference to him/her by name. Such a request will be complied with within 40 days and After Adoption reserves the right to charge the sum of £10 and to limit the number of requests for information in a period of 12 months.

9.3 In the event of any dispute about the accuracy of information relating to an employee, volunteer, student or trustee s/he should raise the issue in writing with his/her manager or the Chief Executive or Human Resources Manager. If the matter cannot be resolved, a marker will be placed against the disputed information in the personal file.