

Data Protection Policy

Version history

|  |  |  |
| --- | --- | --- |
| **Version**  | **Date**  | **Amendments**  |
| **1**  | August 2018  | v.1 – Approved by Adoption West Board of Directors |
| **2**  | October 2019 | v.2 |
| **3**  | October 2020 | v.3 |
| **4**  | October 2021 | v.4 |

Date of next review: October 2022

Electronic Copies

An electronic version of this document is available at <https://www.proceduresonline.com/adoptionwest/local_resources.html>

Comments and Suggestions

We welcome comments and suggestions from readers. They will help us to improve this document in later editions. Please make them to info@adoptionwest.co.uk

Contents

[1. Policy Statement 1](#_Toc529974435)

[2. Purpose 1](#_Toc529974436)

[3. Legal Context and Definitions 1](#_Toc529974437)

[3.1 EU General Data Protection Regulation and Data Protection Act 2018 1](#_Toc529974438)

[4. Scope 3](#_Toc529974439)

[4.1 Context of this policy 3](#_Toc529974440)

[4.2 Personal data held 3](#_Toc529974441)

[5. Responsibilities and Penalties 4](#_Toc529974442)

[5.1 Organisational Responsibilities 4](#_Toc529974443)

[5.2 Individual Responsibilities 4](#_Toc529974444)

[6. Purposes of Processing Personal Data and Fairness 4](#_Toc529974445)

[7. Data Quality, Integrity and Retention 5](#_Toc529974446)

[8. Security 6](#_Toc529974447)

[9. Data Subjects Rights 7](#_Toc529974448)

[9.1 The right to access records – Subject Access Request (SAR) 7](#_Toc529974449)

[10. Disclosure and Sharing 7](#_Toc529974450)

[10.1 Third party access to information 7](#_Toc529974451)

[10.2 Information sharing 8](#_Toc529974452)

[11. Notification 9](#_Toc529974453)

[12. Subject Access Requests and Data Protection Complaints 9](#_Toc529974454)

[13. Implementation 10](#_Toc529974455)

[14. Other related policies 10](#_Toc529974456)

[15. Monitoring and Review 11](#_Toc529974457)

## 1. Policy Statement

Adoption West is fully committed to compliance with the requirements of the EU General Data Protection Regulation and Data Protection Act 2018. The organisation therefore aims to ensure that all employees, contractors, agents, consultants, or partners of the organisation who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the legislation.

## 2. Purpose

The organisation needs to collect and use certain types of information about people with whom it deals in order to perform its functions. This includes information on current, past and prospective employees, suppliers, clients, customers, service users and others with whom it communicates. The organisation is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of the Government departments such as the Police, NHS, DWP, MoJ and other third parties. This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material. There are safeguards to ensure this in the EU General Data Protection Regulation and Data Protection Act 2018.

The organisation regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining confidence between those with whom we deal and ourselves. It is essential that it treats personal information lawfully and correctly.

The purpose of this policy is to explain how the organisation will ensure compliance with the EU General Data Protection Regulation and Data Protection Act 2018. It includes organisational measures and individual responsibilities which aim to ensure that the organisation complies with the Data Protection principles and respects the rights of individuals. This policy provides outline measures and puts in place a structure for monitoring compliance.

Detailed procedures and guidance do not form part of this overarching policy document. The detailed guidance can be accessed via the website and links to relevant documents are included within this Policy document. Other related policies are listed under Section 15.

## 3. Legal Context and Definitions

### 3.1 EU General Data Protection Regulation and Data Protection Act 2018

The EU General Data Protection Regulation (GDPR) and Data Protection Act 2018 govern how information about people (Personal Data) should be treated. It also gives rights to individuals whose data is held. The Regulation came into force on 25 May 2018 and applies to all personal data collected at any time whether held on computer or manual record. The Regulation is enforced by the Information Commissioner’s Office.

The GDPR makes a distinction between personal data and "sensitive” personal data. Sensitive personal data is subject to stricter conditions of processing.

**Personal data** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Sensitive personal data** is defined as personal data consisting of information as to:

Racial or ethnic origin; political opinions; religious or philosophical beliefs; or trade union membership; genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

A **Data Subject** is an individual who is the subject of the data.

A **Data Controller** is an organisation, or person that determines the purposes for which and the manner in which any personal data is to be processed.

A **Data processor** is any organisation or person who processes data on behalf of the data controller.

**Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.

The GDPR contains 6 principles for processing personal data with which organisations must comply.

**Personal data shall be**:

(1) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

**Data subject rights** are:

* The right to be informed that processing is being undertaken.
* The right of access to one’s personal information.
* The right to prevent processing in certain circumstances.
* The right to rectify, block or erase information which is regarded as wrong information.
* The right to have decisions reviewed where they have been made automatically.
* The right to object to receiving marketing information.

## 4. Scope

### 4.1 Context of this policy

This policy applies to all the Staff, Contractors, partners and contractual third parties that use personal data in support of their work on behalf of the organisation.

The policy should be read in conjunction with the Employee Code of Conduct governing the professional conduct and standards of staff.

The policy links with other organisation policies including Freedom of Information and Information Access Policy, Records Management Policy, ICT Security Policy, Email and Internet Use Policies, Human Resources Policies, Criminal Records Bureau Staff checks (Disclosure and Barring Service) Policy and Procedures.

This policy may be supported by other policies and agreements and information sharing protocols for specific areas of work.

This policy may be supported by procedures and guidance for specific areas of work or specific data protection issues, which can be obtained from the Adoption West Procedures on line website ([www.proceduresonline.com/adoptionwest/](http://www.proceduresonline.com/adoptionwest/)).

### 4.2 Personal data held

This policy applies to all processing of personal data held by Adoption West. This includes:

* Personal data processed by Adoption West.
* Personal data controlled by Adoption West but processed by another organisation, on the organisation’s behalf (for example private sector contractors; and Service Level Agreements with voluntary sector organisations).
* Personal data processed jointly by Adoption West and its partners

The policy does not cover personal data held by the Local Authority or the Department for Education which are data controllers in their own right.

Personal data held by Adoption West may be held in many forms including:

* Database records;
* Computer files;
* Emails;
* Paper files;
* Photographs;
* Microfiche and film;
* Website;
* Mobile phones.

Data subjects may include:

* Current, past and prospective employees;
* Suppliers;
* Clients;
* Customers;
* Service users;
* Others with whom the organisation communicates.

##

## 5. Responsibilities and Penalties

5.1 Organisational Responsibilities

Adoption West is a data controller under the EU General Data Protection Regulation and Data Protection Act 2018.

### 5.2 Individual Responsibilities

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

All contractors/ service providers must comply with the policy when using personal data supplied to / held by the organisation to facilitate the Commissioned Service being provided.

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

It is a further offence to sell such data.

Employees who access or use personal data held by the organisation for their own purposes will be in breach of relevant policies of the organisation, including but not limited to the Employee Code of Conduct, Social Media Policy, ICT Security Policy and subject to disciplinary action, which could include dismissal, and may also face criminal proceedings.

## 6. Purposes of Processing Personal Data and Fairness

Adoption West will collect and process personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

The organisation will use a condition of processing as detailed in Article 6(1) of the GDPR of their personal data.

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

When sensitive data is collected, the organisation will use a condition of processing as detailed in Article 9 of the GDPR. These include protecting the vital interests of the data subject or meeting a legal obligation.

In cases where consent is obtained, the consent must be free and informed and may be changed at any time.

Adoption West will ensure that all individuals whose details are processed are aware of the way in which that information will be held, used and disclosed. Individuals will be informed of the likely recipients of the information - whether the recipients are internal or external to the organisation.

This information will be provided when personal data is first collected, whether written or verbal.

When personal data is to be used for a new purpose then the fairness information will be provided to the data subject again and if necessary a new consent will be sought.

People are free to ask for more details about how their personal data is being used at any time and if unhappy about how their data is used may make a complaint.

Any person whose details (including photographs) are to be included on the organisation’s website will be asked to give written consent. At the time the information is included or collected, all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

In accordance with good practice the organisation will share information where appropriate in accordance with formal data sharing arrangements and in accordance with the GDPR and Data Protection Act 2018 principles.

##

## 7. Data Quality, Integrity and Retention

Personal data held will be relevant to the stated purpose and adequate but not excessive.

Adoption West will ensure, as far as is practicable, that the information held is accurate and up-to-date.

If personal data is found to be inaccurate, this will be remedied as soon as possible.

Personal information, such as contact details, may be shared within the organisation where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.

Records may include professional opinions about individuals but employees will not record any personal opinions about individuals.

The Adoption West's use of personal data will comply with the Records Management Policy and Retention Schedules covering every type of organisation record.

Information will only be held for as long as is necessary after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will be done within the requirements of the legislation.

Redundant personal data will be destroyed using the organisation's procedure for disposal of confidential waste and in accordance with retention schedules.

## 8. Security

Any inappropriate, unauthorised access of data, use or misuse of data or failure to comply with ICT security arrangements and policies may result in disciplinary action, including dismissal.

Adoption West will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information.

An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

The organisation has an ICT Security Policy which applies to electronic systems containing personal data.

All information security incidents (however minor) should be reported via the process detailed in the Information Security Incident procedures.

All staff within the organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices or media.

Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

Employees who process personal data out of the organisation (e.g. on another site, on client premises, at home) can only do this with the express consent of their senior manager. Access to personal data outside of the organisation should not be attempted using unsecured access systems (this includes via mobile networks outside of UK unless the network has been checked in advance to be compliant under data protection law).

System testing will only be carried out using personal data where sufficient safeguards are in place and will not be undertaken on live databases accessing live personal sensitive data.

Personal data will not be transferred outside the European Economic Area without the approval of the Data Protection Officer.

## 9. Data Subjects Rights

### 9.1 The right to access records – Subject Access Request (SAR)

Adoption West will ensure that the rights of people about whom the information is held can be fully exercised under GDPR and the Data Protection Act 2018.

The organisation will provide individuals with a copy of the information held about them within one month of receiving a request (subject access). This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

On receiving a request for subject access the organisation will check and require evidence of the identity of the individual and any further information required to isolate the records of that individual.

Where a subject access request has a broad scope, the organisation may ask for more details from the data subject in order to locate the information that is of particular interest.

Where a large volume of information is held, the organisation may seek to make the information available in ways other than providing a copy. This could include arranging an appointment for the data to be inspected within the organisation.

In addition to the personal data itself, the individual will be provided with any supporting information that is needed to understand the data held, and the processing of it.

Where information located as part of a subject access request contains personal data about a third party, information will not be released unless the requirements set out in section 10.1 are met.

The introduction of the right of access to non-personal information held by the organisation under the Freedom of Information Act 2000 may also need to be considered. This is because some requests may be for a combination of personal and non-personal information.

The organisation will comply immediately with a request from an individual to cease sending them marketing or consultation information.

Requests from individuals to correct, rectify, block, or erase information that they regard as wrong information or to stop processing that is causing damage or distress will be considered by the organisation on a case by case basis. The individual concerned will be fully informed of the resulting decision and the reasons for it. Legal advice will be sought by the organisation should a request not be supported, or if considered sensitive/complex before coming to a decision.

An individual wishing to exercise any of their rights under the GDPR or the Data Protection Act 2018 should put their request in writing to Adoption West.

## 10. Disclosure and Sharing

### 10.1 Third party access to information

Where a request for personal data is made by a third party on behalf of the data subject it shall be treated as a subject access request. Evidence is required that the third party is entitled to act in this way, such as a written statement from the data subject or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

Occasionally third party information may form part of the data extracted in response to a subject access request. In deciding whether to release this information, the organisation will consider the following:

* any duty of confidentiality owed to the third party;
* attempts to get consent from the third party;
* any express refusal of consent from the third party;
* the third party’s expectations with respect to that data.

When a request for personal data is made by a third party and not on behalf of the data subject, the organisation shall consider the request under Freedom of Information as well as GDPR and the Data Protection Act 2018. It shall consider whether releasing the personal data would breach any of the Data Protection principles and in particular whether any exemptions under the Act apply. Personal information will not be shared with third parties unless specifically allowed for in law and justified in the specific situation.

The Freedom of Information policy deals with requests for information about third parties, and information will be withheld where disclosing it would breach any of the Data Protection principles. Where a requester does not state a specific reason for requesting the information then the FOI policy should be followed. A response to an FOI request must not take into account the reasons behind the request.

When there is a specific reason for requesting the information, an exemption under the Data Protection Act 2018 may apply. Examples are where information is required for the prevention or detection of crime, apprehension or prosecution of offenders or assessment or collection of tax.

If an appropriate exemption under Data Protection Act 2018 does apply so that the Data Protection principles will not be breached, the organisation will usually comply with the request.

Where the organisation is not convinced that the third party has entitlement to the personal data, or that any exemptions under the Act apply, and that releasing information would breach the Data Protection principles, the personal data will be withheld.

### 10.2 Information sharing

Adoption West promotes information sharing where it is in the best interests of the data subject. However, personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (DPA 2018 exemption exists) to allow the sharing such information.

The organisation will ensure that supporting processes and documentation are made available to professionals so that they understand how to share information safely and lawfully.

Where an employee acting in good faith has shared information in accordance with these supporting processes and documentation, they shall not normally be subject to disciplinary action under section 5.2, hereof.

Sharing large sets of information, or recurrent regular sharing shall be carried out under written agreement to ensure the continued compliance with the GDPR and the Data Protection Act and that additional safeguards can be considered and put in place.

## 11. Notification

The organisation has a notification registered with the Information Commissioner under registration number ZA333965.

The organisation will ensure that this notification is an accurate description of processing carried out by the organisation. The Governing Body will review the notification annually.

The organisation is responsible for submitting this notification to the Information Commissioner.

When the organisation plans to carry out new processing not covered by this notification, will amend the notification (if necessary) within 28 days of processing beginning.

Failure to notify or maintaining an incomplete or inaccurate notification is a criminal offence and may result in a fine.

## 12. Subject Access Requests and Data Protection Complaints

Subject access requests and data protection complaints should be addressed to

Adoption West

Floor 2, Old County Hall

Trowbridge

BA14 8JN

Or email to info@adoptionwest.co.uk

Complaints about the organisation’s processing of personal data and rights under the General Data Protection Regulation and Data Protection Act 2018 will be dealt with in accordance with this Policy. Complaints will be fully dealt with after a formal review. The clarification and review procedure contained in the organisation's Freedom of Information and Environmental Requests Policy and Procedures should be used when dealing with reviews under this policy (Data Protection) and for Freedom of Information and Environmental Information requests.

Individuals have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the General Data Protection Regulation. If individuals are not happy about how we have handled their information they can contact the ICO via the following means:

sent to

Customer Contact

Information Commissioner's Office,

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire,

SK9 5AF

Alternatively visit their website - ico.gov.uk or contact them by phone on 03031231113

The organisation will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.

The organisation will comply with any Information Commissioner Information Notice (to provide answers and information to the Commissioner) or Enforcement Notice (for failure to provide answers or information or for a breach of the Act) sent to the organisation by the Information Commissioner. The Commissioner can also carry out audits, prosecute individuals and organisations and report concerns to parliament.

##

## 13. Implementation

The responsibility for implementation of this policy rests with Adoption West.

The organisation 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 a Data Breach.

On joining the organisation, employees are required to undertake training on Data Protection and ICT Security as part of their induction. They will not be allowed to use the organisation’s network until successfully completing the training.

The Data Protection Officer works with the organisation to maintain the on-going programme of annual training and awareness to maintain a high level of understanding of Data Protection and security among all staff and to communicate any legal or policy changes that occur.

Supporting procedures for this policy have been created and are maintained within the Information Governance, Policy and Guidance pages that are available on the organisation’s website. Appropriate levels of consultation takes place at review time before the governing body approve the changes for implementation.

14. Other related policies

This policy should be interpreted and applied in relation to other related policies. Breach of these policies will automatically breach this policy and this is likely to contravene the General Data Protection Regulation, Data Protection Act 2018 and other legislation. These related policies include, but are not limited to, the following and such other policies as are adopted by the organisation from time to time:

* ICT Security Policy
* Managing Employee Performance
* Subject Access Policy and Procedures
* Record Retention Policy
* Data Sharing Agreements, Protocols and Contracts (various)

## 15. Monitoring and Review

The implementation and effectiveness of this policy will be monitored and reviewed by the organisation.

*This policy will be reviewed at not more than 2-yearly intervals.*