# Data Protection Policy

| | |
|---|---|
| Date reviewed | 31st July 2025 |
| Review date | 31st July 2026 |
| Document type | Security policy |
| Overview | Data management for all business areas as included in the Employee Handbook and incorporates website Privacy Policy. |
| Status | Complete |

Academic Families is commitment to protecting the privacy and security of your personal information. It contains information regarding how we collect and use personal data or personal information about you in accordance with the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force.

Pursuant to that legislation, when processing data we will -

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be lost or destroyed or used for anything that you are not aware of or have consented to (as appropriate)

Academic Families is a data controller. This means that we are responsible for determining the purpose and means of processing personal data relating to you.

Personal data or personal information means any information relating to an identified, or identifiable individual 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.

There are special categories of sensitive personal data, meaning data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sex life or sexual orientation, genetic data, and biometric data which require a higher level of protection.

This data protection compliance statement (privacy notice) applies to current and former employees, workers and contractors.

## Details of information we hold

The kind of data that we will hold includes -

### All

- personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- date of birth
- your photograph
- copy of passport
- gender
- marital status
- next of kin and their details

### Students

- school records and concerns
- medical records

### Employees and volunteers

- any references obtained during recruitment
- details of job duties
- details of health and sickness absence records
- details of holiday records
- information about performance
- details of any disciplinary and grievance investigations and proceedings
- training records
- contact names and addresses
- correspondence with the Company and other information that you have given the Company.
- copy of driving license
- medical and health information

### Employees

- details of terms of employment
- payroll details
- tax and national insurance information
- ether you have a disability or not

The kind of data that that we will process and which falls within the scope of special categories of more sensitive personal information:

- information relating to your religious beliefs
- information about your health, including any medical conditions and disabilities
- information about criminal convictions and offences
- genetic information and biometric data

## Method of collection of personal information

Your personal information is obtained through the application and recruitment process, this may be directly from candidates, via an employment agency or a third party who undertakes background checks. Further information will be collected directly from you when you complete forms at the start of your engagement, employment or when you are accepted as a host, for example, your bank details. Other details may be collected directly from you in the form of official documentation such as your driving license, passport or other right to work evidence. Data may be collected during your engagement with us to enable its continued existence or development.

Personal data is kept in secure folders within our IT system.

## Processing information about you

We will only administer personal information in accordance with the lawful bases for processing. At least one of the following will apply when we process personal data:

- Consent - you have given clear consent for us to process your personal data for a specific purpose
- Contract - processing is necessary for a contract we have with you, or because we have asked you to take specific steps before entering a contract
- Legal obligation - the processing is necessary for us to comply with the law (not including contractual obligations)
- Vital interests - the processing is necessary to protect someone's life
- Public task - the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law
- Legitimate interests - the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect your personal data which overrides those legitimate interests.

## Lawful basis for processing your personal information

We consider that the basis for which we will process the data contained in the list above - **Details of Information we hold about you** - is necessary for the performance of the contract we have with you and to enable us to comply with our legal obligations. Occasionally, we may

process personal information about you to pursue legitimate interests of our own or those of third parties, provided there is no good reason to protect your interests and your fundamental rights do not override those interests.

The circumstances in which we will process your personal information are listed below.

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc
- responding to requests from third parties such as a reference request or mortgage approval
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave, pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access

There may be more than one reason to validate the reason for processing your personal information.

## Lawful basis for processing special categories of sensitive data

Special categories of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- Consent - you have given clear consent for us to process your personal data for a specific purpose
- Contract - the processing is necessary for a contract we have with you, or because we have asked you to take specific steps before entering into a contract
- Legal obligation - the processing is necessary for us to comply with the law (not including contractual obligations) and meets the obligations under our data protection policy
- Vital interests - the processing is necessary to protect someone's life.
- Public task - the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law and meets the obligations under our data protection policy e.g. in the case of equal opportunities monitoring
- Legitimate interests - the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect your personal data which overrides those legitimate interests e.g. to assess your capacity to work on the grounds of ill health

Occasionally, special categories of data may be processed where you are not capable of giving your consent, where you have already made the information public or in the course of legitimate business activities or legal obligations and in line with the appropriate safeguards.

Examples of the circumstances in which we will process special categories of your particularly sensitive personal information are listed below (this list is non-exhaustive):

- in order to protect your health and safety in the workplace
- to assess your physical or emotional fitness to work
- to determine if reasonable adjustments are needed or are in place
- to monitor and manage sickness absence, family leave or other absences from work (including time off for dependents)
- to administer benefits
- In order to fulfil equal opportunity monitoring or reporting obligations

Where appropriate, we may seek your written authorisation to process special categories of data. Upon such an occasion we will endeavour to provide full and clear reasons at that time in order for you to make an informed decision. In any situation where consent is sought, please be advised that you are under no contractual obligation to comply with a request. Should you decline to consent you will not suffer a detriment

## Information about criminal convictions

Information regarding criminal convictions may be processed in accordance with our legal obligations. Occasionally we may process such information to protect yours, or someone else's interests and you are not able to give your consent, or we may process such information in cases

where you have already made the information public. Such information may be sought as part of the recruitment process or in the course of your employment with us. Where we process information regarding criminal convictions, we will adhere to the guidelines currently in force regarding data security and data retention as determined by the appropriate governing body.

We anticipate that we will process information about criminal convictions.

## Automated decision making

We do not anticipate that any of our decisions will occur without human involvement. Should we use any form of automated decision making we will advise you of any change in writing.

## Sharing data

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. This includes, for example, your manager for their management of you, the HR department for maintaining personnel records and the payroll department for administering payment under your contract of employment.

It may be necessary for us to share your personal data with a third party or third party service provider (including, but not limited to, contractors, agents or other associated/group companies) within, or outside of, the European Union (EU). Data sharing may arise due to a legal obligation, as part of the performance of a contract or in situations where there is another legitimate interest (including a legitimate interest of a third party) to do so.

The list below identifies which activities are carried out by 3rd parties on our behalf:

- payroll
- pension providers/administrators
- IT services
- legal advisors
- HR advisors
- security
- insurance providers

Data may be shared with 3rd parties in the following circumstances:

- in the process of regular reporting activities regarding our performance
- with regards to a business or group reorganisation, sale or restructure
- in relation to the maintenance support and/or hosting of data
- to adhere with a legal obligation
- in the process of obtaining advice and help in order to adhere with legal obligations

If data is shared, we expect 3rd parties to adhere and comply with the GDPR and protect any data of yours that they process. We do not permit any 3rd parties to process personal data for their own reasons. Where they process your data it is for a specific purpose according to our instructions.

We anticipate that we will not transfer data to other countries.

## Data Security

As part of our commitment to protecting the security of any data we process, we have put the following measures in place: all company files are securely saved on our Microsoft Office 365 password protected system and individual devices are protected by Endpoint Data Protection services. If you would like further details please contact the Managing Director.

Any data that is shared with 3rd parties is restricted to those who have a business need, in accordance with our guidance and in accordance with the duty of confidentiality.

### Your data security responsibilities

You are responsible for ensuring that any personal data that you hold and process as part of your job role is stored securely.

You must ensure that personal information is not disclosed orally, in writing, via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the Disciplinary Procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected on our network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and, where possible, it should be locked away out of sight, for example in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight, for example in the boot of a car.

### Notifying breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches -

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

### Investigation and notification

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by a Director.

We will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

We will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

### Record of breaches

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under the Data Protection Act 2018. It records the facts relating to the breach, its effects and the remedial action taken.

## Data Retention

We anticipate that we will retain your data for as long as we need it but for no longer than is necessary for the purpose for which it was collected.

We have considered the following in order to decide the appropriate retention period:

- quantity
- nature

- sensitivity
- risk of harm
- purpose for processing
- legal obligations

At the end of the retention period, upon conclusion of any contract we may have with you, or until we are no longer legally required to retain it, it will be reviewed and deleted, unless there is some special reason for keeping it. Occasionally, we may continue to use data without further notice to you. This will only be the case where any such data is anonymised, and you cannot be identified as being associated with that data

## Your Rights in Relation to Your Data

We commit to ensure that any data we process is correct and up to date. It is your obligation to make us aware of any changes to your personal information.

In some situations, you may have the;
Right to be informed - this means that we must tell you how we use your data, and this is the purpose of this privacy notice.

Right to request access - you have the right to access your data that we hold. You may, within a period of one month of a written request, inspect or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data.

Right to request correction - if any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it.

Right to request erasure - if you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it.

Right to object to the inclusion of any information - in situations where we are relying on a legitimate interest (or those of a third party) you have the right to object to the way we use your data where we are using it.

Right to request the restriction of processing - you have the right to ask us to stop the processing of data of your personal information. We will stop processing the data (whilst still holding it) until we have ensured that the data is correct.

Right to portability - you may transfer the data that we hold on you for your own purposes.

Right to request the transfer - you have the right to request the transfer of your personal information to another party.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact the Managing Director.

## Consequences of your failure to provide personal information

If you neglect to provide certain information when requested, it may affect our ability to enter into or continue with an employment contract with you, and it may prevent us from complying with our legal obligations.

## Change of purpose for processing data

We commit to only process your personal information for the purposes for which it was collected, except where we reasonably consider that the reason for processing changes to another reason and that reason is consistent with the original basis for processing. Should we need to process personal information for another reason, we will inform you of this and advise you of the lawful basis upon which we will process.

Important note: We may process your personal information without your knowledge or consent, in compliance with the above Lawful Basis for Processing Your Personal Information

In the event that you enter into an employment contract with us, any information already collected may be processed further in accordance with our data protection policy in the employee handbook.

## Who to contact

Lorna Clayton MBE, Managing Director

lorna@academicfamilies.com 07734 849554

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.