Academic Guardians UK

Data Protection Policy

Academic Guardians UK Ltd (AGUK) will comply with all statutory requirements of The Data Protection Act 2018 ("the Act") by taking all reasonable steps to ensure the accuracy and confidentiality of such information.

London Registered Office
Kemp House, 152-160 City Road, London, EC1V 2NX

Telephone
+44 (0) 203 515 8880
+44 (0) 203 815 7943

Mobile
+44 (0) 7931 954 106
+44 (0) 7823 321 993

Email
info@academic-guardians.co.uk

Online
www.academic-guardians.co.uk

Policy owner	Updated	Review date
Andrew Kettle	January 2020	January 2021

Academic Guardians UK - Data Protection Policy

Data Protection Statement

Academic Guardians UK Ltd (AGUK) will comply with all statutory requirements of The Data Protection Act 2018 ("the Act") by taking all reasonable steps to ensure the accuracy and confidentiality of such information. AGUK needs to gather and use certain information about individuals. These can be members, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to the meet the AGUK's data protection standards, and to comply with the legislation.

This data protection policy ensures AGUK:

- Complies with data protection law and follows good practice
- Protects the rights of staff, members and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of data breach.

The Information Commissioner's Office

The Information Commissioner's Office (ICO) is "the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals" (ICO website). It is responsible for administering the provisions of the Data Protection Act 2018; the Freedom of Information Act 2000 (not relevant to AGUK); and the General Data Protection Regulation 2018. The Act requires every data controller who is processing personal information to register with the ICO (unless exempt). AGUK is registered with the ICO as a data controller, and this is renewed annually.

The ICO publishes a Register of data controllers on their website, on which AGUK (Academic Guardians UK Ltd) is listed, registration number ZA050126. AGUK's data controller is Dawn Kettle.

The Data Protection Act 2018

An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes. When carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.

The Act protects individuals' rights concerning information about them held on computer and in any AGUK personnel files and databases. These rules apply regardless of whether data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Freedom of Information Act 2000

The Freedom of Information Act 2000 provides public access to information held by public authorities, in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

General Data Protection Regulation 2018

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. The GDPR places greater emphasis on the documentation that data controllers must keep demonstrating their accountability. Compliance requires organisations to review their approach to governance and how they manage data protection as a corporate issue.

AGUK will handle and protect all information in line with data protection principles set out in the Act. Under the Act, anyone processing data must comply with the eight principles of good practice for data protection, as detailed below:

Data will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive in relation to the purpose(s) for which they are processed
- Accurate and kept up to date
- Not kept longer than necessary
- Processed in accordance with the data subject's rights under the Act
- Secure and protected. Appropriate technical and organisational measures are in place to protect data from unauthorised or unlawful processing and from accidental loss, damage or destruction.
- Not be transferred to a country or territory outside of the European Economic Area (EEA) unless we can be assured there is an adequate level of protection for the rights and freedoms of the data subjects

This AGUK Data Protection policy applies to personal data as defined by the Act – that is, data from which a living individual can be identified, either from data alone, or from that data and other information that is held by the data controller. This includes information held on computer, paper files, photographs etc.

Responsibilities

This policy applies to the main office of AGUK, all staff, local coordinators, homestay hosts, drivers and volunteers of AGUK, and all contractors and other people working on behalf of AGUK. The scope of the policy applies to all data held by AGUK relating to identifiable individuals. Everyone who works for AGUK has responsibility for ensuring data is collected, stored and handled appropriately – all must ensure personal data is handled and processed in line with this policy and data protection principles. The Directors are ultimately responsible for ensuring that AGUK meets its legal obligations.

The data controller (Dawn Kettle) is responsible for:

- Keeping the Directors updated about data protection responsibilities, Reviewing all data protection procedures and policies
- Arranging data protection training if required
- Handling data protection queries from those working for and with AGUK
- Dealing with requests from individuals relating to the data AGUK holds about them
- Assisting with any agreements with third parties that may handle sensitive data
- Working with AGUK's IT contractors to ensure that all systems, services and equipment used for storing data meet acceptable security standards, including ensuring regular checks, scans and updates to ensure security hardware and software are functioning properly.

The purpose of the Act is to make sure that personal data is used in a way that is fair to the individual and protects their rights, while enabling organisations to process personal data in pursuit of their legitimate aims.

Lawful Basis for processing personal data

AGUK has identified three categories under which processing may take place:

Consent:	the individual has given clear consent for AGUK to process their personal data for a specific purpose.
Legal obligation:	the processing is necessary for AGUK to comply with the law (not including contractual obligations).
Vital interests:	the processing is necessary to protect someone's life.

AGUK works directly with parents and agents (representing parents both in the UK and abroad), staff, homestay host families and local co-ordinators. These parties are asked to sign a contract, giving their consent for AGUK to use the data that is requested and supplied in a manner compliant with the needs of GDPR when they first appoint AGUK as placement agent or education guardian; wish to become an employee; local co-ordinator or homestay host family.

Processing personal data of children

Upon registration with AGUK we request documents as per **Appendix A** from the students and in particular request copies of the current passport and BRP where applicable and accepts this as bona fide documents containing wholly accurate information. No further checks are carried out by AGUK on the data contained therein. AGUK is aware when a passport/BRP expires and will update the records with new information as it becomes available.

AGUK also requests the NHS medical numbers and doctors surgery details once the students have arrived in the UK.

Homestay Host Families with children over the age of 16 or becming 16 will be required to provide the necessary documentary evidence to enable AGUK to obtain a valid DBS certificate.

Staff guidelines

- Personal data should not be shared informally – it should not be sent by general email – this form of communication is not secure.
- Personal data must be encrypted before being transferred electronically. AGUK uses an email server called 'Stay Private '. With click-and-PIN access, TLS connections, AES-256 encryption and multi-factor authentication, StayPrivate enables AGUK to exchange data with clients in a convenient, secure and GDPR-compliant manner. Outlook 365 is the way to access AGUK emails outside of Outlook or other email client/software. Only people with access details are permitted to access the AGUK webmail system. The webmail is password protected.
- Employees should not save copies of personal data to their own computers/laptops – personal data should always be accessed and updated via the central copy of any data – the AGUK SharePoint server.
- Employees should keep all data secure, taking sensible precautions and following these guidelines.
- Strong passwords must be used, and never shared.
- Personal data should not be disclosed to unauthorised people, either within AGUK or externally.
- Data should be regularly reviewed and updated if found to be out of date. If no longer required, it should be deleted and/or disposed of.
- When not in use, paper format data or files (for instance, DBS applications) should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for instance, on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When working with personal data, employees should ensure computer/laptop screens are always locked when left unattended.
- Where data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- If data is stored on removable media (for instance, a CD or USB), these should be kept locked away securely when not in use.
- Data should only be stored on designated drives and servers, and/or approved cloud computing services (AGUK uses Azure Microsoft Platform & SharePoint sites with varying access level settings dependant on roles and responsibilities – AGUK retains the privacy and use settings of the information's stored in this way)
- Data should be backed up frequently, and backups should be tested periodically.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Personal data should never be saved directly to laptops or other mobile devices like smart phones or tablets, unless encrypted.

Use of Photographs and Videos

AGUK has a Photgraphy and Images Policy which aims to ensure that every reasonable effort is made to minimise risk of inapporporaiate captue and distribution of photos and images. The policy also extends to ensureing that the appropriate permission levels are obntained and recorded. This policy is made available on the AGUK website and Sharepoint portal for Staff, students, parents, local coordnaitors and homestay host families. Hard copies are also available on request.

Sharing personal data

Student data is only shared with schools and potential host families, except in the event of a safeguarding risk or medical emergency where it may be shared with local services such as medical or social care.

Host Family data is sent to prospective students' parents/agents where the student is expected to stay with the host family.

AGUK does not share any data with any 3rd party without permission and no data is ever sold.

AGUK may also use/process collected information to:

- Contact parents, homestay hosts, students, referees, schools and local authorities
- Undertake administrative functions (for example, HR, contact referees, share feedback, obtaining Visas, arranging private fostering requirements, transporting students and parents)
- Process DBS applications
- Compile marketing lists (e.g. for newsletter and conferences)
- Handle complaints
- Conduct research
- Understand people's views and opinions (for example, via feedback forms)
- Comply with legal and regulatory obligations (AEGIS, HMRC, ICO)
- Marketing of AGUK products and services through the use of testimonials and photographs in various mediums including booklets and social media sites carefully working within the procedural guidelines set out in this policy, with particular emphasis on the use of photographs and videos.

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, AGUK will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Directors, and by taking legal advice where necessary. If on the rare occasion, we need to share data, we will only use data anonymously. If personal information is shared, it will be done so in line with the Act. You are entitled to know why and how we are sharing your personal information and the organisation or individual receiving your personal information will be required to protect your information in line with the Act.

Protecting your information

Academic Guardians UK Ltd – Data Protection Policy

The directors of AGUK, through the company polices determine the procedures for, and implement through training, how information should be collected, shared, stored and deleted. AGUK has appropriate technical and organisational measures in place to protect your information. Paper files are locked away securely and electronic files are protected by access rights (strong passwords are used) set at a server level. All electronic files are stored, using AES 256 password strength encryption. AGUK's server is only accessible by the IT director when connected to the internet/networks, using encrypted log in details.

Data accuracy

The law requires AGUK to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees and people working with AGUK, who work with data, to take reasonable steps to ensure it is kept accurate and as up to date at possible.

- Data should be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated, for instance, details can be updated when a member calls.
- AGUK will make it easy for data subjects (for instance, homestay hosts and students and parents) to update their own information AGUK holds about them, for instance, via the AGUK website and A+ Portal.
- Any data inaccuracies should be corrected as soon as discovered, for instance if a member can no longer be reached on their stored telephone number, this should be removed from the database).

Data protection risks

This policy helps to protect AGUK from data security risks including:

- Breaches of confidentiality, for instance: information being given out inappropriately
- Failing to offer choice, for instance: all individuals should be free to choose how the company uses data relating to them
- Reputational damage, for instance: the company could suffer if hackers successfully gained access to sensitive data.

Accessing your information

Under the Act, an individual is entitled to ask AGUK:

- For a copy of the personal information held by AGUK
- For any inaccuracies to be corrected
- How to gain access to such data
- How they are meeting their data protection obligations

Such requests are known as 'Subject access requests'. Such requests should be made either via email or via the post.

Email requests should be addressed to the data controller at office@academic-guardians.co.uk. Postal requests should be submitted to:

Academic Guardians UK Ltd | Capital Offices, Kemp House, 152-160 City Road, London, EC1V 2NX.

Last updated: January 2020

Academic Guardians UK Data Controller, Capital Offices, Kemp House, 152-160 City Road, London, EC1V 2NX.

There is no administration charge for any subject access request. The data controller will aim to provide the relevant data within 14 working days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Logging and recording of communications with individuals

AGUK may log communications with you for the purposes described earlier in this policy.

Links to other websites on the AGUK website

Our website includes links to other websites (for example: to other organisations dealing with boarding students, government departments and agencies). We are not responsible for the data protection and privacy practices of these organisations, including their website. This Data Protection Policy applies to AGUK only.

Cookies

Refer to AGUK Privacy Policy on the AGUK website.

Providing information

AGUK aims to ensure that individuals are aware that their data is being processed, and that they are understanding:

- How the data is being used
- How to exercise their rights

To these ends, a copy of this policy which sets out how data relating to individuals is used by AGUK can be available on request. This policy is also available on the AGUK website and internal intranet Shaperpoint sites and Homestay Host Family portals.

If you have any questions about this policy, please contact the Data Controller at AGUK via email at office@academic-guardians.co.uk or by post at:

Academic Guardians UK Data Controller,

Capital Offices, Kemp House, 152-160 City Road, London, EC1V 2NX

Academic Guardians UK Ltd – Data Protection Policy

Policy prepared by: Andrew Kettle - Director

Approved: January 2020

Policy became operational on: 12 January 2020

Next review date: January 2021

Appendix A	Student	Host Family	Parents (Overseas)
Example Data:			
Full name (including title, forename(s), family name)		✓	✓
ID documents - passport, drivers licence, birth certificates, BRP – Visas	✓	✓	✓
Contact information	✓	✓	✓
Qualifications/experience		✓	
Date of birth	✓	✓	
Information relevant to HR (for example: C.V.s, interview notes, referee details,		✓	
DBS reference numbers		✓	
Social Services background checks		✓	
References		✓	
Medical Information including consent authority	✓	✓	
Banking Details for making and receiving payments	✓	✓	✓
School names and personnel, medical centre information	✓		
School year group, form tutor details	✓		
Main language for correspondence	✓		✓
Level of guardianship service provided	✓		✓
Homestay host family information and annual update notes		✓	
Dates of homestays and school visits with feedback information		✓	
Safeguarding monitoring records		✓	
Whether private fostering assessment has been undertaken by the Local Authority		✓	
Details of venues (name, location, address, contact details)	✓		✓
Feedback forms	✓	✓	
Photographs (for example, students, homestay hosts, parents, staff and	✓	✓	✓
Financial Payments		✓	✓
Hobbies, Interests, Allergies and preferences	✓	✓	