OXFORD GUARDIANS

OXFORD GUARDIANS
DATA PROTECTION POLICY

1. Introduction

1.1 Oxford Guardians is a guardianship company providing educational support and homestay facilities to international boarding students studying in the UK.

1.2 This policy supports the legal requirements of the UK General Data Protection Regulation (GDPRUK), tailored by the amended Data Protection Act 2018, which places certain obligations on the Company, its staff and those who process data on our behalf. The EU GDPR was incorporated directly into UK law as the UKGDPR. We have students based in the EU and therefore the EUGDPR applies to services supplied to them. The EU approved adequacy decisions on 28 June 2021 this means data from the EU can flow as before in the majority of circumstances.

1.3 Breach of this policy may result in the cessation of contract.

1.4 We do not have a formal Data Protection Officer but the member of staff responsible for data Protection is Kevin Bacon who may be contacted by email at Kevin@oxfordguardians.com or by telephone at +44(0)1604859331. This policy will be reviewed on an annual basis. It may, however, be amended in advance of such date in response to changes in future legislation.

1.5 The Company is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

1.6 Changes to data protection legislation shall be monitored and implemented to remain compliant with all requirements.

1.7 The principles of the Data Protection Act shall be applied to all data processed and shall be:

- Processed fairly, transparently and lawfully.
- Obtained only for lawful purposes, will not be further used in any manner incompatible with those original purposes.
- Accurate and kept up to date
- Adequate, relevant, and limited to what is necessary to achieve the contractual and legal purposes of the company.
- Not kept for longer than is necessary for those purposes
- Processed in accordance with the rights of data subjects under the DPA

Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction, or damage

- In the case of EU residents or citizens, data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

2. Organisational Scope

2.1 This is a corporate policy and applies to former, current, and potential employees and associates of Oxford Guardians (OG). Moreover, this policy forms part of an agreement with any organisation which may be engaged to process personal data on behalf of the Company in the future.

2.2 We are a data controller and data are processed by our staff in the UK, and protections provided by the suppliers of our improved database rolled out in September 2021, by inlocoparentis.org. However, for the purposes of IT conference hosting and file maintenance some information is located on Dropbox and Zoom servers which are GDPR compliant. We will not collect any information from you that we do not need to provide and oversee our services.

2.3 Our data processor is **Inlocoparentis.org (ILP).** We signed a contract with that company in advance of the move to their data platform in September 2021. We have conducted an **information audit** and we currently collect and process the following information:

- Personal identifiers, contacts, and characteristics i.e. full name, Date of Birth, gender, nationality, visa Biometric Residence Permit, passport and contact details of parents, schools, students, employees, contractors and agents.
- Personal images for identification. Normally taken from a Passport provided by the or directly by the subject.
- Other files relevant to the provision of our service for example boarding cards for flights.
- Summary information for homestays.
- Family members and other contact information relevant to the supply of guardianship services.
- Medical, including allergies and medications.
- Cultural data.
- Financial, including invoice and pricings.
- Academic data such as school reports, notifications, and disciplinary matters.
- Lifestyle such as likes, dislikes, sports, hobbies
- Employee, contractors /consultants vetting and recruiting information.
- Proof of Right to Work (RTW) in the UK such as a UK Passport or other documentation such as BRP, Home office letter of indefinite right to remain or a visa vignette.
- Proof of Identity and address documentation for DBS processing. Only the RTW document is retained the remainder is deleted after DBS processing is complete.

3. Definitions

This section includes all necessary definitions of GDPR terms which are not in everyday usage or where there is a need to be precise.

3.1 Consent

Consent means offering people genuine choice and control over how we use their data. Consent must be freely and explicitly given to be valid.

3.2. Data Subject

Data subject means “an individual who is the subject of personal data collection”. A data subject must be a living individual.

3.3 Information Commissioner’s Office (ICO)

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. The ICO enforce the law regarding information

compliance legislation.

3.4 Lawful Processing for Legitimate Interests

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.5 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

3.6 Personal data breach

Personal information data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. We are legally obliged to report breaches that are likely to result in a risk to the rights and freedoms of individuals to the ICO and individuals will have to be notified directly by the Company.

3.7 Processing of Personal Data

Processing, in relation to information or data, means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including –
organisation, adaptation or alteration of the information or data.
retrieval, consultation or use of the information or data.
disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.

3.8 Records Disposal

The Company will retain records only if they are needed and then, when they are no longer needed, permanently delete them or dispose of them in some other way, e.g., by permanent and irretrievable deletion via a verified commercial service.

4. How we store information post the withdrawal from the EU

4.1 We are our own data processors and are based in the UK with in-house data storage, and or in Dropbox. However, our partner , **InLoco Parentis (ILP**) has servers situated within the EU and UK. Data is transferred between the client web browsers and the servers using SSL encryption. ILP and Dropbox use strong ciphers and flags all authentication cookies as secure. Identifiable personal data at rest is stored on ILP /Dropbox servers using 256-bit Advanced Encryption Standard (AES) encryption and is disaggregated. Data backups and incremental backups of stored data are performed hourly. Our data processor also maintains a reliable service and in the rare event that a server is not available to access they can switch to a duplicate backup server to restore the service. But see 4.2 below. In the unlikely event of a breach, we will send the subject and ICO a breach notification as required by applicable law. We maintain incident response policies and procedures, including a breach notification process, and we are aware that it is incumbent upon us to notify persons affected as needed.

4.2 The data protection provisions set out in the Withdrawal Agreement apply unless full adequacy decisions are adopted by the EU, when UKGDPR will obtain. Accordingly, we will comply with EU data protection law when transferring the data of EU subjects from the EU to the UK, including that acquired before 31 December 2020. The so called 'Frozen GDPR'. OG will ensure that we continue to operate in tandem under GDPR and UK DPA law. However, OG has very few client's resident in the EU and in any event the GDPR UK and amended DPA2018 practically mirrors EU legislation in this regard.

4.3 Photocopies of Passports and other documents needed to prove the Right To work in the UK are held on an external hard drive separated from the Drop box or ILP servers and held at rest (offline)in locked containers.

5. How we get the information and why we have it

The personal information we process is provided to us directly by parents on registration or by students of 13 years or older and by employees or contractors during recruiting and vetting procedures and to prove identity for the Disclosure and Barring Service (DBS).

6. Under the General Data Protection Regulation UK (GDPRUK) and DPA 2018, the lawful basis we rely on for processing this information are:

6.1 Your informed consent and you may remove your consent at any time. You can do this by contacting kevin@oxfordguardians.com or by telephone at +44(0)1604859331. However, the removal of consent to hold essential data may mean that we cannot fulfill our obligations to you regarding the academic and parochial care of a student.

6.2 We have a contractual obligation to you which may only be achieved by holding this data.

6.3 We have a legitimate interest.

7. What we do with the information we have.

We use your personal data to:

7.1 Provide and manage the guardianship services that the contract between us describes.

7.2 Update student educational records

7.3 Provide information to parents, local guardians, agents and teachers about placement, events, lessons, timetables, transport and student progress.

7.4 Examine data and its processing to improve the operation of our business.

7.5 Comply with legal and regulatory obligations, and to follow guidance and best practice following changes to the rules of governmental and regulatory bodies

7.6 Enable management and auditing of our business operations including accounting

7.7 Monitor and to keep records of our communications with parents, students, agents, our staff, and educational establishments.

7.8 Send you personalised information by SMS, WhatsApp, email, phone, or post about the provision of our service. For example,

- information about forthcoming school events relevant to the student or reporting information.
- To share information, as needed, with Universities, colleges and schools and our Guardians, homestay, teachers or service providers.

8. When do we share your personal information with other organisations?

8.1 We share information only with third parties detailed in paragraph 7 immediately above and at 8.2 below. and to comply with legal and regulatory obligations.

8.2 The intention to share data relating to individuals or to a third party organisation or person outside of our company such as schools and colleges shall be clearly defined within our Terms and Conditions together with the details of the basis for sharing. Data may be shared with external parties in circumstances where it is a legal requirement to provide such information.

9. How long is your personal information retained by us?

9.1 Unless we explain otherwise to you, we will hold your personal information for as long as we have reasonable business needs to do so such as providing our services to you and managing our operations. Thereafter, we will retain information for as long as someone could bring a claim against us; and/or for retention periods in line with legal and regulatory requirements or guidance.

9.2 We are obliged to see the original DBS certificates to confirm applicants' details, the clearance is enhanced, the certificate number and date of issue and that the children's barred list has been checked. We keep a copy for only such time as an associate is actively operating on our behalf. We will destroy these immediately on an employee or contractor ceasing to be associated, with us although we will keep a record of the DBS certificate number and the date issued. When checking the currency of an associate enrolled on the DBS update service we conduct an 'employers' check using Name Certificate number and DOB at https://secure.crbonline.gov.uk/crsc/check?execution=e1s1

10. What should you do if your personal information changes?

10.1 You should tell us so that we can update our records by contacting us at the address above. We will then update your records.

10.2 Do you have to provide your personal information to us? No, but we may be unable to provide you with our services if you do not provide certain information to us.

11. Do we do any monitoring or automated decision-making involving processing your personal information?

We do not.

12. Your data protection rights

Under data protection law, you have rights including:

12.1 **Your right of access** - You have the right to ask us for copies of your personal information.

12.2 **Your right to rectification** - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

12.3 **Your right to erasure** - You have the right to ask us to erase your personal information.

2.4 **Your right to restriction of processing** - You have the right to ask us to restrict the processing of your information.

12.5 **your right to object to processing** - You have the the right to object to the processing of your personal data.

12.6 **Your right to data portability** -You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at Info @Oxfordguardians.com or by Post to Oxford Guardians, The HIF, Gayton, Northamptonshire, NN7 3EY if you wish to make a request.

13. Photographs and Video:

13.1 We may wish to capture Images of staff, Guardians, Homestay families and Students at appropriate times and, with the express permission of the subjects, use them as part of promotional material on the company website or other company marketing materials.

13.2 Unless explicit prior consent from parents/students/staff has been given, the company shall not utilise such images for publication or communication to external sources.

14. Responsibilities of Core Staff, Local Guardians, and Homestay Providers.

14.1 Core Staff

- Must ensure that all student information folder data passed to local guardians is passed via ILP, by hand or by encrypted e-mail. The company has a Gmail business account which has this facility built in and all core staff and Local guardians are provided with an Oxford Guardians Email address from this account.

- In response to COVID 19 restrictions, staff working from home are provided with company laptop computers and mobile telephones. The computers have a Norton Anti-Virus suite installed comprising anti-virus, malware detection, anti- phishing, firewall protection and VPN modules. Staff must use these devices for company business and ensure the AV suite is enabled.

- Staff must not download unapproved apps or services on to these devices.

- Documents containing personal data must be cleared from desks and locked away after work.

14.2 Local Guardians

Are to protect the personal or sensitive student's data and ensure reports and information passed to the central office via email must be done so using the company account and with the data encrypted as described in 14.1 above.

14.3 Homestay Providers Are to be made aware of and briefed to protect the personal and sensitive nature of Student's information including cultural, dietary, and medical information passed to them to fulfil homestay arrangements as well as email addresses and telephone contact numbers.

15. Notification:

15.1 Our data processing activity is registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO at:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

15.2 Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

15.3 Oxford Guardians employees or associates who discover a data breach must report this immediately to the responsible staff member, Kevin Bacon, who will investigate to discover the extent and severity of the data loss.

15.4 Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and if significant within 72 hours to the ICO.

16. Data Disposal:

16.1 The company recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. Data held on devices are to be permanently and irretrievably deleted. Company issued devices have 'File Shredder 'installed which will delete irretrievably. Data held on other devices such as homestay host personal PC must also be deleted. The company recommend three free apps.. They are: File Shredder, Eraser, and Freeraser

16.2 Time expired devices, thumb drives, CDs, tape, or other electronics no longer required shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. Paper records will be destroyed by fire on company property by the officer responsible for Data Protection.

16.4 Disposal of IT assets holding data shall follow ICO guidance:
https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

17. How to complain.

In the first instance data subjects should contact Kevin Bacon by email at kevin@oxfordguardians.com or by telephone at **+44(0)1604859331**. Or by Post to **Oxford Guardians, The HIF, Gayton, Northamptonshire, NN7 3EY** You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113

Reviewed By	date	Peer Review by	
KT Bacon	09/12/2020	SA Bacon	20/12/2020
KT Bacon	12/02/2021	SA Bacon	14/02/2021
KT Bacon	03/12/2022	SA Bacon	03/12/2022