Oxford Guardians

Cybersecurity Policy

In all its dealings with international students and their families and UK schools, Oxford Guardians (OG) will follow the general standards laid out by The Association for the Education and Guardianship of International Students (AEGIS) in their Code of Practice, which are as follows:

- To promote and provide best and legal practice in the guardianship and hosting of all international students at schools, colleges and universities, particularly those under 18 years of age.
- To respect and support the rights, religions and customs of the international student.
- To uphold the stated ethos and values of the school attended by students in our guardianship.
- To comply with the Children Acts 1989 and 2004 and the Education Act (2002) and adhere to the guidance of the Keeping Children Safe in Education 2024 (KCSIE) updated September 2024.
- To ensure all international students have 24 hour emergency contact with a responsible adult in the UK.
- To put in place arrangements which maintain appropriate contact with the international student, the overseas parents and guardianship family and to ensure all appropriate records are up to date.
- To provide both pastoral and educational support as outlined in any literature and agreements.
- To adhere to the AEGIS grievance procedures.
- To have appropriate insurance for guardianship arrangements and to comply with UK legislation.

1. Introduction

This Cybersecurity Policy defines the framework for managing the cybersecurity risks associated with the operations of Oxford Guardians(OG). OG is committed to protecting the confidentiality, integrity, and availability of its digital systems, networks, and the sensitive data of students, families, and staff, in compliance with relevant legislation in England and Wales.

2. Purpose

The purpose of this policy is to:

- Safeguard personal and academic data in line with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- Define responsibilities for ensuring cybersecurity practices across the Company.
- Prevent data breaches and cyberattacks that may compromise the security of sensitive information.

Ensure compliance with cybersecurity best practices and legal obligations.

3. Scope

This policy applies to:

- All employees, contractors, and third-party vendors who have access to the Company's networks, systems, or data.
- All devices, platforms, and systems, including email, online storage, and communication tools used to support guardianship services.
- All data relating to students, families, employees, and partners stored or processed by the Company.

4. Cybersecurity Responsibilities

- Director: Accountable for ensuring Oxford Guardians implements robust cybersecurity governance, compliance, and risk management.
- DPO or Officer Responsible for Data Protection: We do not have a DPO but do have an officer responsible for advising on data protection and privacy issues in compliance with the UK GDPR and the Data Protection Act 2018, and managing incident responses
- Inlocoparentis (ILP) Customer Relationship Manager: Responsible for the technical aspects of securing the CRM database.
- Employees and Contractors: All personnel must follow the cybersecurity procedures outlined in this policy, including reporting potential security incidents.

5. Data Protection

- Compliance with Data Protection Laws: All data processing activities must adhere to the Data Protection Act 2018 and the UK GDPR, ensuring the protection of students' and families' personal and academic data.
- Data Access and Encryption: Sensitive personal data is held on the company database, ILP, and held secure and encrypted when stored and when transmitted. Access should be restricted to authorized personnel only based on their job roles.
- Data Retention: Oxford Guardians will only retain personal data for as long as it is necessary for business purposes or as required by law. Data must be securely deleted when no longer required.

6. Information Security Practices

- Network Security: Oxford Guardians must employ appropriate security measures, such as firewalls, intrusion detection systems, and regular network monitoring, to protect against unauthorized access and cyberattacks.
- Multi-Factor Authentication (MFA): MFA must be implemented for accessing external systems containing sensitive information or personal data. This includes email, cloud storage, and internal platforms.

Patch Management: All systems, software, and devices must be regularly updated to address known vulnerabilities and apply security patches.

- Anti-malware and Antivirus Software: All company devices are protected with up-to-date commercial anti-malware and antivirus software, and scanning should be conducted regularly. Guardians and Homestay Hosts are briefed on the measures and protocols to be adopted to keep student data safe.

7. Employee and Contractor Training

- Cybersecurity Awareness Training: All employees and contractors will complete cybersecurity awareness training upon hiring and participate in refresher briefings annually. Topics will include data protection, phishing, password security, and social engineering tactics.
- Phishing and Social Engineering: Employees are educated on how to recognize phishing emails, social engineering attacks, and other tactics used to compromise personal or company data.
- Incident Reporting: Employees must immediately report any suspected security incident, such as a data breach or cyberattack, to the DPO.

8. Incident Response

- Incident Response Plan: Oxford Guardians will maintain a detailed incident response plan to address potential data breaches, cyberattacks, or other security incidents. This plan will include:
- Procedures for containing and mitigating the impact of the incident.
- Notification protocols to inform affected parties (e.g., students, parents, staff) and relevant authorities in accordance with legal requirements (e.g., the Information Commissioner's Office (ICO)).
- A post-incident review to identify lessons learned and improve future security practices.
- Breach Notification: In the event of a data breach, Oxford Guardians will notify the ICO within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms, as per the UK GDPR. Affected individuals will be notified if necessary.

9. Third-Party Vendors and Service Providers

- Third-Party Risk Management: Oxford Guardians will assess the cybersecurity practices of all third-party vendors, including cloud service providers such as ILP and Dropbox, to ensure that they meet the approved cybersecurity and data protection standards.
- Data Processing Agreements (DPAs): We are our own data controllers and are based in the UK with minimal in-house low level data storage or processed in Dropbox and InLoco Parentis (ILP). However, our partner, 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 flag all authentication cookies as secure. Identifiable personal data at rest is stored on ILP 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. All contracts with third-party vendors must include a DPA that specifies the security measures they must take to protect the Company's data in line with the UK GDPR.
- Ongoing Audits: Regular cybersecurity audits and assessments will be conducted to ensure that third-party vendors continue to comply with contractual obligations and regulatory requirements.

10. Acceptable Use of Technology

- Personal Devices: Local Guardians and Homestay Hosts necessarily use personal devices for work-related activities (BYOD). Devices must be secured with appropriate access controls, virus checking apps and firewalls. Associates are regularly briefed on maintaining patches to keep apps and devices secure. Student data is not held on BYOD but in ILP in access restricted folders

- Social Media and Information Sharing: Employees must not share sensitive or confidential information about students, families, or Oxford Guardians staff on personal social media or online forums. Any work-related social media activity must comply with the Company's guidelines.

11. Compliance and Legal Considerations

Oxford Guardians will ensure compliance with all relevant laws, regulations, and standards, including:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- The Computer Misuse Act 1990
- The Privacy and Electronic Communications Regulations (PECR)

12. Enforcement and Disciplinary Actions

Employees and contractors who fail to comply with this policy may face disciplinary action, which could include termination of employment or contractual relationships. Serious violations may also result in legal consequences.

13. Policy Review and Updates

This policy will be reviewed annually or whenever there are significant changes to the Company's operations, systems, or relevant laws. Employees will be notified of any updates or changes to the policy.

This cybersecurity policy ensures that Oxford Guardians is taking a proactive and legally compliant approach to safeguard personal, academic, and operational data. Oxford Guardians is dedicated to maintaining a secure and trustworthy environment for all students and families.

Review date	Reviewer	Appointment
17/12/2024	KT Bacon	DSL