**Data Protection Impact Assessment (DPIA)**

*(for help and guidance in completing this form please contact the Information compliance team at* *DPA@westminster.ac.uk**)*

|  |  |
| --- | --- |
| DPIA authors | Gunter Saunders |
| Service / School | Digital Engagement and Library Services |
| Title | Learnwise – chatbot for Blackboard trial |
| ISS reference (where applicable) |  |
| Date completed | 20/12/2024 |

|  |  |
| --- | --- |
| **Screening question – are you…..***Please answer yes/no to each questions. If you’re answer is ‘yes’ to any of the below, please complete the form. If ‘no’ please submit your completed form to* *DPA@westminster.ac.uk* | **Yes/No** |
| Evaluating or scoring individuals (including profiling and predicting)? | **No** |
| Conducting automated decision-making? | **No** |
| Systematically monitoring individuals or groups? | **No** |
| Processing any sensitive personal data? | **No** |
| Processing personal data on a large scale? | **Yes** |
| Matching or combining datasets containing personal data? | **No** |
| Processing personal data of vulnerable people? | **No** |
| Using new or changed technology solutions (including use of a new third party suppliers)? | **Yes** |
| Using innovative technology solutions (including any use of artificial intelligence)? | **Yes** |
| Transferring personal data outside of the European Union (including use of cloud solutions)? | **No** |
| Restricting an individual(s) from exercising their rights under data protection legislation? | **No** |

|  |
| --- |
| **Context**Provide a description and the context of the personal data processing. What are the intended outcomes? Why and how is the personal data processed? By which organisation(s)?Whose personal information will be processed e.g. students, alumni, third parties?What volume of information will be processed and how often?Will you be processing children’s data? |
| Implementing Learnwise's AI chatbot functionality within the University's Virtual Learning Environment (VLE).The work we are doing involves integrating Learnwise's AI chatbot through LTI connection to provide 24/7 academic support to students. The system will be piloted across selected courses from each academic School, affecting approximately 2,000-3,000 users. LearnWise.ai is designed specifically for higher education institutions, offering AI-driven student support that integrates seamlessly with existing educational platforms. The Learnwise AI Assistant platform has been built from scratch for Higher Education student and faculty support.**Data Processing Organizations:**- Primary processor: LearnWise.ai - Sub-processors: AWS and Azure for cloud infrastructure and AI services**Users and Scope:**- Primary users: University students and faculty- Secondary users: Teaching assistants, VLE administrators- Public access users (if placed on public pages)- Total initial scope: 2,000-3,000 users during pilot**Data Processing Volume and Patterns:**- Average usage: 4-5 interactions per student per month- Typical session length: 8-22 messages- High-usage cases: Some users exceed 500+ messages- Frequency: Daily/weekly usage expected**Data Flow and Integration:**- Data collection via LTI framework and Blackboard APIs- Pulls course data, calendar information, and enrolment data- Conversation history accessible to: • University admin team via admin panel • Individual users can access their own conversations while logged in- Data retention: 90 days post-contract completion or upon request**Purpose of Processing:**1. Primary purposes: - Providing immediate responses to student queries - Supporting academic and administrative inquiries - Enhancing student support services2. Secondary purposes: - Analysing question patterns to improve chatbot efficiency - System performance monitoring and enhancement - Service optimization based on usage patterns**Privacy Controls:**- Clear privacy notices within chatbot interface- User guidelines for appropriate usage- Opt-out mechanism for students- Clear complaint and rectification procedures- No processing of data related to individuals under 18**Data availability and deletion:**- Data accessible during contract duration- Deletion within 90 days of contract completion- On-request deletion available |

|  |
| --- |
| **Types of personal data***Please state what personal data you will be processing.*  |
| **Personal data**  | **Yes/No** | **Special category personal data** | **Yes/No** |
| Name | Yes | Race | No |
| Address | No | Ethnic origin | No |
| Email address | Yes | Political opinions | No |
| Telephone numbers | No | Religious or philosophical beliefs | No |
| Date of birth | No | Trade union membership | No |
| Gender | No | Genetic data | No |
| Financial information e.g. card number, salary, income | No | Biometric data | No |
| Education and qualifications | Yes | Health data | No |
| Location data (including mobile phone tracking and IP addresses) | No | Sex life | No |
| Residency data/eligibility to live in the UK | No | Sexual orientation | No |
| Images or recorded footage | No |  |  |
| Crime data e.g. criminal convictions or allegations, witness statements | No |  |  |
| Unique identifiers e.g. passport number, NHS number | Yes |  |  |
| Other (please state);Questions from students (could relate to any subject) |  |  |  |

|  |
| --- |
| **Lawful basis for processing personal data***To process personal data organisations need to identify a lawful basis. Further guidance can be found* [*here*](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/) *for personal data and* [*here*](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/#:~:text=Article%209(2)(a,UK%20GDPR%20standard%20for%20consent.) *for special category personal data.*  |
| **Basis for processing personal data** | **Basis for processing special category personal data** |
| **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose |  | **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose |  |
| **Contract:** the processing is necessary for a contract you have with the individual |  | **Made public by the data subject:** the individual has disclosed the data themselves |  |
| **Legal obligation:** the processing is necessary for you to comply with the lawPlease state which legislation applies: |  | **Employment, social security and social protection law:** processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field |  |
| **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law | X | **Legal claims and judicial acts:** necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |  |
| **Vital interests:** the processing is necessary to protect someone’s life |  | **Vital interests:** the processing is necessary to protect someone’s life |  |
| **Legitimate interests:** the processing is necessary for your legitimate interests unless there is a good reason to protect the individual’s personal data which overrides those interests. This cannot apply where a public authority is processing data to perform official tasks |  | **Health or social care:** necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems |  |
|  |  | **Substantial public interest:** necessary for reasons of substantial public interest, on the basis of Domestic Law which shall be proportionate to the aim pursued |  |
|  |  | **Not-for-profit bodies:** processing is carried out in the course of its legitimate activities with appropriate safeguards and relates solely to the members or to former members of the body |  |
|  |  | **Public health:** necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care |  |
|  |  | **Archiving, research and statistics:** for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |  |

|  |
| --- |
| **Systems and Storage**What software will be used to manage the personal data?If this is software provided by a third party, please provide details?Has a contract been drawn up with the third party which includes data protection clauses?Where in the world is the data held?Will this system link with any others or export data? How will access to the system be controlled?What backup and recovery procedures will be put in place? |
| **Systems and Storage****Software and Data Management:**Data flows through the system as follows:1. Questions submitted via Blackboard VLE interface using LTI authentication2. User context (course, role, permissions) passed securely to LearnWise3. Questions processed through content safety screening, context enrichment, and AI processing4. Responses returned to VLE and stored encrypted5. Chat history accessible to individual users and authorized administrators**Technology Stack:**- LearnWise AI Assistant platform - AWS and Azure cloud services for infrastructure - All processing in EU data centers- Integration via LTI and Blackboard APIs**Security & Access Controls:**- Role-based access control (RBAC) with principle of least privilege- Multi-factor authentication for admin access- Data encrypted in transit (TLS 1.3) and at rest (AES-256)- Regular penetration testing and vulnerability assessments- Activity monitoring and audit logging- Access limited to authorised administrators with documented procedures**Data Protection:**- Processing confined to EU/EEA region- Sub-processors bound by SCCs and DPAs- Data retention: 90 days post-contract or upon request- Regular compliance audits (SOC 2, ISO 27001, GDPR)- Privacy by design principles implemented**Backup & Recovery:**- Automated daily encrypted backups- Geographic redundancy within EU- RPO: 24 hours / RTO: 4 hours- Regular disaster recovery testing- 99.9% system availability target- Incident response aligned with GDPR requirements |

|  |
| --- |
| **Technical diagram**Use diagrams and text to map and describe the data flows |
| LearnWise's system processes data through the following secured flow:1. Access & Authentication- User access via Blackboard LMS using LTI protocol- Authentication through LMS credentials and OAuth2- All traffic secured via HTTPS and load balancers2. Data Processing- Queries processed through load-balanced EU-based servers- Specialized job queues handle content processing and embedding- Real-time chat processing with course context integration3. Data Storage- All databases hosted in EU data centers- Encryption at rest and in transit |

|  |
| --- |
| **Retention**What will the retention period be?How will data be disposed of when no longer needed?How will data be preserved (if required)? |
| 1 academic year |

|  |
| --- |
| **Identification of privacy risks***Please use this table to document any risks you have identified* |
| **Risk ID** | **Privacy risk***e.g. No privacy policy or statement covering personal data collections.* | **Impact***What impact in relation to a person would the risk have – High, Medium or Low* | **Likelihood***What is the likelihood of this risk having that impact if left uncontrolled – High, Medium or Low* | **Mitigation***What controls will be put in place to mitigate the risk?* | **Due date** | **Managed by**Insert name |
| 01 | Potential processing of personal information within student questions | Medium | Medium | Clear user guidelines about not sharing personal information in queries |  |  |
| 02 | Unauthorised access to accumulated question data | Low | Medium | Limited administrative access and European data storage |  |  |
| 03 | Vulnerabilities in LTI connection | Low | High | Standard LTI security protocols and regular security testing |  |  |
| 04 |  |  |  |  |  |  |
| 05 |  |  |  |  |  |  |

|  |
| --- |
| **Consultation***Please state who has been consulted regarding this personal data processing?* |
| **Team/Role** | **Name** |
| Project manager  | Gunter Saunders |
| Data management and security | Thierry Delaitre |
| Supplier representative | Ian Haugh Learnwise |
| University Business Representative | Micael Berhane (LIDE) |
| University Business Relationship Manager | N/A |
| Business Sponsor | Ian Wilmot |
| Information Compliance Team | Nicola Cooke |

|  |
| --- |
| **Data Protection Officer Assessment***When you have completed this form, please send it to* *DPA@westminster.ac.uk**. The organisations Data Protection Officer will assess the privacy implications in accordance with the legislative requirements below. You may be asked to provide further information.*  |
| **DPA principle** | **Yes/No** | **Comment** | **Action required** |
| Processed lawfully, fairly and in a transparent manner |  |  |  |
| Collected for specified, explicit and legitimate purposes |  |  |  |
| Relevant and limited to only what is necessary |  |  |  |
| Accurate and where necessary kept up to date |  |  |  |
| Retained only for as long as necessary |  |  |  |
| Processed in an appropriate manner to maintain security |  |  |  |

|  |
| --- |
| **Signoff** |
| **Name** |  |
| **Date** |  |