HK HOUSE OF KNOWLEDGE Ltd

DATA PROTECTION POLICY

House of Knowledge (HK) is a Platform with an ambitious mission to enable change through access to international professional and general educational opportunities via partnerships with academic and professional bodies. We are providing wide range of learning and personal interaction, communication to create and exchange knowledge for the benefit of society. As such the Platform needs to obtain and process certain information about our staff, contractors, learners and participants of the activities to allow us to register and organise events, programmes, and carry out other essential activities.

The information we collect is used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we comply with the relevant legislation indicated below.

The Platform's need to communicate and share personal data with the partners to ease and facilitate learning process of the participants of various programmes also presents some data protection risks. The platform needs to collect, use and share personal information about programmes' and certifications candidates/students, staff and other individuals in order to deliver services, exercise its responsibilities and duties of care as an employer and provider of services and fulfil its legal and contractual obligations. In doing so the platform must comply with the Law on *Protection of Personal Data in Ukraine* (http://zakon5.rada.gov.ua/laws/show/2297-17) and the latest instructions *On procedure for processing data* (http://www.ombudsman.gov.ua/ua/page/secretariat/docs/legislation/tipovij-poryadok-obrobki-personalnix-danix.html) and equivalent legislation, such as the *Processing of Personal Data (Protection of the Individual) Law* or *Directive of the European Union* (95/46), acting in other jurisdictions in which the platform operates.

These laws require the platform to collect, process, store and protect personal information and control how it is used in accordance with the legal rights of the data subjects - the individuals whose personal data is held.

All staff, candidates, students and other data subjects are entitled to know

- Why information is gathered, stored and where the body, requesting the information, is located;
- Which third parties have access to their personal data;
- How to gain access to the own personal information;
- How to keep it up to date;
- What the Platform is doing to comply with its legal obligations

PURPOSE

This policy and its supporting procedures and documents aim to ensure that the platform complies with its obligations as a Data Receiver/Controller/User under all applicable

legislations, and processes all personal data in compliance with the Data Protection Principles. In summary, these state that personal data shall:

- Be obtained and processed fairly and lawfully
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Be kept for no less than a time span identified by relevant laws for every respective area.
- Be kept safe from unauthorised access, accidental or deliberate destruction or unauthorised change.

Misuse of personal data, whether accidental or deliberate loss or disclosure to third parties, presents significant legal, financial and reputational risks and loss of recruitment income. In order to manage these risks, this policy sets out responsibilities for all managers, staff, partners and contractors and anyone else that can access or use personal data in their work with the platform.

The policy incorporates framework of governance and accountability for data protection by maintaining • Confidentiality: protecting information from unauthorised access and disclosure

- Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion
- Availability: ensuring that information and associated services are available to authorised users whenever and wherever required

SCOPE

What information is included in the Policy: This policy applies to all personal data created or received in the course of business in all formats, of any age. Personal data may be held or transmitted in paper and electronic formats or communicated verbally in conversation or over the telephone.

Who is affected by the Policy Data subjects: These include, but are not confined to: prospective applicants, applicants to programmes and posts, current and former learners and students, alumni, current and former employees, family members where emergency or next of kin contacts are held, workers employed through agencies, external researchers, visiting scholars and volunteers, potential and actual donors, customers, conference delegates, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors.

Users of personal data: The policy applies to anyone who obtains, records, can access, store or use personal data in the course of their work for the platform. Users of personal data include

employees and students of the partners of the platform, contractors, suppliers, agents, platform partners and external researchers and visitors.

Where the Policy applies: This policy applies to all locations from which platform personal data is accessed including home use. As the platform operates internationally through arrangements with partners in other jurisdictions the remit of the policy shall include such overseas collaborations and international activities and shall pay due regard to non-European legislation that might be applicable.

OBJECTIVES

The platform will apply the Data Protection Principles to the management of all personal data throughout the information life cycle by adopting the following policy objectives. We will:

- Use proportionate privacy impact assessment to identify and mitigate data protection risks at an early stage of project and process design for all new or updated systems and processes that present privacy concerns and in managing upgrades or enhancements to systems used to process personal data
- Adopt data minimisation: we will collect, disclose and retain the necessary minimum personal data for the minimum necessary time for the purpose /
- Process personal data fairly and lawfully
- Treat people fairly by using their personal data for purposes and in a way that they would reasonably expect
- Get informed consent in the manner prescribed by law
- Inform data subjects what we are doing with their personal data by explaining in a clear and accessible way: What personal data we collect, For what purposes and why we need it; How we use it and how we will protect their personal data; to whom we may disclose it and why; where relevant, what personal data we publish and why

We will publish this information on our portal and where appropriate in printed formats.

We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them. We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them such as home addresses.

Where we process personal data to keep people informed about platforms' activities and events we will provide in each communication a simple way of opting out of further marketing communications. In this way we will provide accountability for our use of personal data and demonstrate that we will manage people's data in accordance with their rights and expectations.

Upholding individual's rights as data subjects

This means that we will uphold their rights to

- Get access to their personal data, responding to requests for their own personal data (subject access requests) in a fair, friendly and timely manner
- Object to processing that is likely to cause or is causing unwarranted and substantial damage or distress
- Object to decisions being taken by automated means
- Have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances

Protection of personal data

This means that we will

- Control access to personal data so that staff, contractors and other people working on platform business can only see such personal data as is necessary for them to fulfil their duties
- Require all staff and contractors, who have access to personal data in the course of their work to complete basic data protection training, relevant to their specific roles
- Set and monitor compliance with security standards for the management of personal data
- Take all reasonable steps to ensure that all suppliers, contractors, agents and other external bodies and individuals who process personal data for the platform enter into our Data Processor Agreements and comply with instructions On procedure for processing data
- Maintain Data Sharing Agreements with educational partners and other external bodies with whom we may need to share student, staff personal data to deliver shared services or joint projects to ensure proper governance, accountability and control over the use of such data
- Manage all subject access and third party requests for personal information about staff, students and other data subjects in accordance with our Procedures for responding to requests for personal data
- Make appropriate and timeous arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for platform business and under applicable legislation, whichever occurs later.
- Retain personal data only as long as required

LINES OF RESPONSIBILITY

All users of platform information are responsible for

- undertaking relevant training and awareness activities provided by the platform to support compliance with this policy
- Taking all necessary steps to ensure that no breaches of information security result from their actions
- Reporting all suspected information security breaches or incidents promptly so that appropriate action can be taken to minimise harm.
- Informing the platform of any changes to the information that they have provided to the platform in connection with their employment or studies, for instance, changes of address

The Attorney General of the platform bears ultimate accountability for the platform's compliance with data protection law.

The Academic Director has senior management accountability for information governance including data protection management and for providing proactive leadership to instil a culture of information security within the platform through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

All Heads of Programmes, Projects and Professional Services divisions are responsible for implementing the policy within their business areas, and for adherence by their staff.

The Assigned Information Services provider is responsible for ensuring that centrally managed IT systems and services take account of relevant data protection risks and are integrated into the information security management system and for promoting good practice in IT security among relevant staff.

The team members of Student Support and Relations Department are responsible for ensuring that controls to manage the physical security of the platform take account of relevant data protection risks and are integrated into the information security management system.

MONITORING AND EVALUATION

The Attorney General and The Academic Director under support of Assigned Information Services provider will monitor new and ongoing data protection risks and update the information security risk register.

The Head of Students Support and Relations Department will liaise with Assigned Information Services provider to ensure that IT security risks related to data protection are prevented, captured on the register and escalate and resolve where necessary. The Head is responsible for escalating major risks arising from a breach of information security, or other major issues that affect strategic and operational risks, promptly to relevant partners and management.

The Attorney General is also responsible for meeting any reporting requirements of external regulatory bodies.

As part of the platform's internal audit programme, the Attorney General will instruct the platform's Internal Auditors to audit the management of information security risks and compliance with relevant controls, as required.

IMPLEMENTATION

This policy is implemented through the development, implementation, monitoring and review of the component parts of the platforms information security management systems.

These include

- Staff employed undertake information risk assessments to identify and protect confidential and business critical information assets and IT systems

- Coordination of effort between all team and Assigned Information Services provider to integrate, IT, physical security, people, information management, and risk management and business continuity to deliver effective and proportional information security controls

- Review and refresh of all relevant policies and procedures

- Generic and role specific training and awareness

- Embedding information governance requirements into procurement and project planning

- Information security incident management policies and procedures

- Business continuity management

- Monitoring compliance and reviewing controls to meet business needs

RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

This policy forms part of an interconnected set of Platform Policies and procedures. Effective data protection and information security controls are essential for compliance with the Code of Laws of Ukraine and other relevant law in all jurisdictions in which the Platform operates.

Legislation that places specific data protection, information security and record keeping obligations on organisations includes, but is not limited to:

- the Law on Protection of Personal Data in Ukraine (http://zakon5.rada.gov.ua/laws/show/2297-17)

- instructions On procedure for processing data (http://www.ombudsman.gov.ua/ua/page/secretariat/docs/legislation/tipovij-poryadok-obrobki-personalnix-danix.html)

- the Processing of Personal Data (Protection of the Individual) Law, 2001 (where applicable)

Any further queries should be forwarded to info@k-house.in.ua with indication “Data Protection Request” in the subject field