Data Protection Policy

February 2020

Kindi Education
DATA PROTECTION POLICY
CONTENTS

Section **Page**

1. INTRODUCTION

Kindi Education must comply with the European Union General Data Protection Regulation (GDPR), UK Data Protection Act, 2018 and other relevant legislation protecting privacy rights. As a learning institution and its constituent legal entities are UK Data Controllers, and also Data Processors for certain activities, the territorial scope of this legislation, and therefore of this policy, applies to all processing of personal data by and for Kindi Education, regardless of where the processing takes place.

These data protection laws require Kindi Education to 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 data subjects are entitled to know

- Their rights under data protection law and how to use them
- What Kindi Education is doing to comply with its legal obligations under data protection law

Misuse of personal data, through loss, disclosure, or failure to comply with the Data Protection Principles and the rights of data subjects, may result in significant legal, financial and reputational damage. This may include penalties of up to €20 million or 4% of worldwide annual turnover for serious breaches of the law, claims for compensation and loss of recruitment and research income.

In order to manage these risks, this policy sets out responsibilities for all managers, employees, contractors, and anyone else who can access or use personal data within Kindi Education.

2. PURPOSE

2.1 This policy and its supporting procedures and guidance support Kindi Education's compliance with its obligations as a Data Controller and where applicable, a Data Processor under data protection law.

Kindi Education is responsible for, and must be able to demonstrate, compliance with the following Data Protection Principles ("accountability").

In summary, these state that personal data shall be:

Processed lawfully, fairly and in a way that is transparent to the data subject (“lawfulness, fairness and transparency”);

- Collected or created for specified, explicit and lawful purposes and not be further processed in a manner that is incompatible with those purposes. (“purpose limitation”);

- Adequate, relevant and limited to what is necessary for those purposes (“data minimisation”);

- Accurate and kept up to date (“accuracy”);

- Retained in a form that can identify individuals for no longer than is necessary for that purpose (“storage limitation”);

- Kept safe from unauthorised access, processing, accidental or deliberate loss or destruction (“integrity and confidentiality”).

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is compatible with the purpose and storage limitation principles, subject to appropriate safeguards for the rights and freedoms of the data subjects.

Under data protection law Kindi Education must also:

- Proactively inform data subjects about its data processing activities and their rights under the law,

- Meet its legal obligations as a data controller or processor, including data protection by design and default, data protection impact assessment, maintaining records of processing activities, measures to ensure the security of processing, handling of data breaches; designation and role of the Data Protection Officer,

- Allow personal data to be transferred to other countries only if it maintains the same level of protection for the privacy rights of the data subjects concerned.

2.2 This policy sets out a framework of governance and accountability for data protection compliance across Kindi Education.

- 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 Resilience: the ability to restore the availability and access to

information, processing systems and services in a timely manner in the event of a physical or technical incident

3. OBJECTIVES

Kindi Education will apply the Data Protection Principles and the other requirements of data protection law to the management of all personal data throughout the information life cycle by adopting the following policy objectives.

3.1 Process personal data fairly and lawfully

This means that we will

- Only collect and use personal data in accordance with the lawful conditions set down under the GDPR;

- Document each condition we rely on; maintain this information within a formal set of Records of Processing Activities; regularly review and update these records and make them available to the Information Commissioner's Office, other supervisory authorities and data subjects on request;

- Treat people fairly by using their personal data for purposes and in a way that they would reasonably expect;

- Ensure that if we collect someone's personal data for one purpose e.g. to provide advice on study skills, we will not reuse their data for a different purpose that the individual did not agree to or expect e.g. to promote goods and services for an external supplier

- Rely on consent as a condition for processing personal data only where

    - We first obtain the data subject's specific, informed and freely given consent, and
    - The data subject gives consent, by a statement or a clear affirmative action that we document, and
    - The data subject can withdraw their consent at any time without detriment to their interests.

3.2 Inform data subjects what we are doing with their personal data

This means that, at the point that we collect their personal data, we will explain to data subjects in a clear, concise and accessible way

- The identity and contact details of Kindi Education and the Data Protection Officer,

- What personal data we collect,

  For what purposes we collect and use their data,

- What lawful conditions we rely on to process data for each purpose and how this affects their rights,

- Whether we intend to process the data for other purposes and their rights to object,

- The sources from which we obtain their data, where we have received the data from third parties,

- Whether we use automated decision making, including profiling, and if so the impact on data subjects and their rights to object,

- Whether they need to provide data to meet a statutory or contractual requirement and if so, the consequences of not providing the data,

- Our obligations to protect their personal data,

- To whom we may disclose their data and why,

- Which other countries we may we may send their data to, why we need to do this and what safeguards apply in each case,

- Where relevant, what personal data we publish and why,

- How data subjects can update the personal data that we hold,

- How long we intend to retain their data,

- How to exercise their rights under data protection law.

We will publish this information on our website 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 Kindi Education activities and events we will provide in each communication a simple way of opting out of further marketing communications.

In these ways 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.

3.3 Uphold individual's rights as data subjects

This means that we will uphold their rights to:

Obtain a copy of the information comprising their personal data, free of charge within one month of their request,

- Have inaccurate personal data rectified and incomplete personal data completed,

- Have their personal data erased when it is no longer needed, if the data have been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data,

- Restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the Kindi Education no longer needs to keep personal data but the data subject needs the data for a legal claim,

- Data portability; where a data subject has provided personal data to the Kindi Education by consent or contract for automated processing and asks for a machine-readable copy or have it sent to another data controller,

- Object to and prevent further processing of their data for Kindi Education's legitimate interests or public interest unless the Kindi Education can demonstrate compelling lawful grounds for continuing,

- Prevent processing of their data for direct marketing,

- Stop the Kindi Education processing data obtained for online services such as social media, where consent for the processing was previously given by or on behalf of a child, who withdraws their consent

- Object to decisions that affect them being taken solely by automated means,

- Claim compensation for damages caused by a breach of data protection law.

3.4 Apply "data protection by design and default" principles to all our personal data processing

This means that we will:

- Use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate privacy risks at each stage of every project or initiative involving processing personal data and in managing upgrades or enhancements to systems and processes used to process personal data,

- Adopt data minimisation: we will collect, disclose and retain the minimum personal data for the minimum time necessary for the purpose,

Anonymise personal data wherever necessary and appropriate, e.g. when using it for statistical purposes, so that individuals can no longer be identified.

3.5 Protect personal data

This means that we will use appropriate technical and organisational measures to:

- Control access to personal data so that staff, contractors and other people working on Kindi Education business can only see such personal data as is necessary for them to fulfil their duties,

- Require all Kindi Education, contractors, students and others who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles,

- Set and monitor compliance with security standards for the management of personal data as part of the Kindi Education 's wider framework of information security policies and procedures,

- Reduce risks of disclosure by pseudonymising personal data where possible,

- Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working away from Kindi Education, for instance through provision of a secure Virtual Private Network, encryption and cloud solutions,

- Take all reasonable steps to obtain assurance that all suppliers, contractors, agents and other external parties who process personal data for the Kindi Education will comply with auditable security controls to protect our data and enter into our Data Processor Agreements,

- Maintain Data Sharing Agreements with educational partners and other external bodies with whom we may need to share personal data to deliver academic programmes, shared services or joint projects to ensure proper governance, accountability and control over the use of such data,

- Where transferring personal data to another country outside the European Union put in place appropriate agreements and auditable security controls to maintain privacy rights,

- Ensure that our students are aware of how data protection law applies to their use of personal data in the course of their studies or research and how they can take appropriate steps to protect their own personal data and respect the privacy of others,

- 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 timely arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for Kindi Education business.

3.6 Retain personal data only as long as required

This means that we will:

- Apply the Kindi Education records retention policies to keep records and information containing personal data only so long as required for the purposes for which they were collected.

Some Kindi Education records containing personal data are designated for permanent retention as archives or for scientific, historical and statistical purposes. When managing access to archives containing personal data we will apply appropriate technical and organisational measures to safeguard the rights and freedoms of the data subjects concerned:

- Apply exemptions to public rights of access to information as appropriate in accordance with the data subjects' rights to privacy,

- Redact personal data, e.g. by pseudonymisation,

- Withhold access to specific categories of record, such as student records, for the lifetime of the student and their identifiable next of kin.

3.7 Manage any breaches of data security promptly and appropriately

This means that we will take all necessary steps to reduce the impact of incidents involving personal data by following the Kindi Education's Information Security Incident Management Policy and Procedures

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will liaise with the Information Commissioner's Office and report the breach, in line with regulatory requirements, within 72 hours of discovery. The Data Protection Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

4. SCOPE

4.1 What information is included in the Policy

This policy applies to all personal data created or received in the course of Kindi Education business in all formats, of any age. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone.

4.2 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 students, alumni, current and former employees, family members where emergency or next of kin contacts are held, workers employed through temping agencies, members of the Court and members of the Committees of the Court, research subjects, 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 Kindi Education. Users of personal data include employees and students of Kindi Education, contractors, suppliers, agents, Kindi Education partners and external researchers and visitors.

4.3 Where the Policy applies

This policy applies to all locations from which Kindi Education personal data is accessed including home use.

5. LINES OF RESPONSIBILITY

5.1 All users of Kindi Education information are responsible for

- Completing relevant training and awareness activities provided by the Kindi Education 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 to hr@kindieducation.com so that appropriate action can be taken to minimise harm,
- Informing the Kindi Education of any changes to the information that they have provided to Kindi Education in connection with their employment or studies, for instance, changes of address or bank account details.

5.2 The CEO, as the Chief Executive Officer of Kindi Education, has ultimate accountability for the Kindi Education 's compliance with data protection law.

5.3 The Data Protection Officer is responsible for

- Informing and advising senior managers and all members of the Kindi Education community of their obligations under data protection law;
- Promoting a culture of data protection, e.g. through training and awareness activities;
- Reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across Kindi Education;
- Advising on data protection impact assessment and monitoring its performance;
- Monitoring and reporting on compliance to Kindi Education, the Audit and Risk Committee and other relevant committees and boards;
- Maintaining Records of Processing Activities;
- Providing a point of contact for data subjects with regard to all issues related to their rights under data protection law;
- Investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence;
- Acting as the contact point for and cooperating with the Information Commissioner's Office on issues relating to processing.

5.6 - All Kindi Education employees are responsible for implementing the policy within their business areas, and for adherence by their staff. This includes

- Assigning generic and specific responsibilities for data protection management;
- Managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data is necessary for them to fulfil their duties;
- Ensuring that all staff in their areas of responsibility undertake relevant training provided by the Kindi Education and are aware of their responsibilities for data protection;
- Ensuring that staff responsible for any locally managed IT services liaise with Kindi Education staff to put in place equivalent IT security controls;
- Assisting the Data Protection Officer in maintaining accurate and up to date records of data processing activities.

6. MONITORING AND EVALUATION

6.1 Kindi Education (if not the Data Protection Officer) will monitor new and on-going data protection risks and update the relevant Kindi Education risk register, reporting this promptly as required to Kindi Education Chief Executive.

7. IMPLEMENTATION

This policy is implemented through the development, implementation, monitoring and review of the component parts of Kindi Education.

These will require

- The Data Protection Officer of Kindi Education to review and update information risk assessments and records of processing activities and take necessary actions to identify and protect personal data and systems used to process the data;
- Coordination of effort between relevant specialities and professional specialists to integrate IT, physical security, people, information management, risk management and business continuity to deliver effective and proportionate information security controls;
- Review and refresh of all relevant policies and procedures;
- Generic and role specific training and awareness;
- Embedding privacy by design and default and related 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.

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1 Legal Requirements and external standards

Effective data protection and information governance controls are essential for compliance with U.K. and Scottish law and other relevant legislation in all jurisdictions in which Kindi Education operates:

The EU GDPR, Regulation (EU) 2016/679

All current UK Legislation is published at http://www.legislation.gov.uk/

UK Information Commissioner's Office (ICO)
Guidance on the GDPR
Privacy and Electronic Communications Regulations
Data Protection Statutory Codes of Practice and Guidance

9. DEFINITIONS

Information The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, biometric or genetic data, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

Personal Data Information in any format that relates to an identified or identifiable living person. An identifiable living person is someone who can be identified directly or indirectly from an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Although the GDPR and the Data Protection Act 2018 apply only to living people, the scope of this policy also includes information about deceased individuals. This is because disclosure of information about the deceased may still be in breach of confidence or otherwise cause damage and distress to living relatives and loved ones.

Special categories of Special categories of Personal Data (formerly known

Personal Data	as sensitive personal data) (as defined in Articles 9 and 10 of the GDPR) are personal data relating to an identifiable person's: a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) membership of a trade union; e) physical or mental health or condition; f) sexual life or sexual orientation; g) proven or alleged offences, including any legal proceedings and their outcome h) genetic or biometric data when processed to identify that individual In addition, the Kindi Education definition of High-Risk Confidential Information includes the following personal data: Any other information that would cause significant damage or distress to an individual it was disclosed without their consent, such as bank account and financial information, marks or grades.
Data protection law	Relevant privacy legislation includes but is not confined to European Union General Data Protection Regulation 2016/679 (GDPR), UK Data Protection Act, 2018, UK Privacy and Electronic Communications Regulations, and equivalent legislation.
Data Controller	An organisation which determines the purposes for which personal data is processed and is legally accountable for the personal data that it collects and uses or contracts with others to process on its behalf.
Data Processor	In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	A living person whose personal data is held by the Kindi Education or any other organisation.
Natural person	A living person, not a "legal person" i.e. a company or other legal entity.

Processing	Any operation performed on personal data, such as collecting, creating, recording, structuring, organising, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data.
Confidential information	The definition of confidential information can be summarised as: ▪ Any personal information that would cause damage or distress to individuals if disclosed without their consent ▪ Any other Information that would prejudice the Kindi Education's or another party's interests if it were disclosed without authorisation More details can be found in our information security classification scheme.
Information Security Management System (ISMS)	"That part of the overall management system based on a business risk approach to establish, implement operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources." BS ISO/IEC 27001: Information Security
Anonymisation	Irreversible removal of personal identifiers from information so that the data subject is no longer identifiable. Anonymised information therefore no longer falls within the definition of personal data.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure

that the personal data are not attributed to an identified or identifiable person. Pseudonymised data is therefore re-identifiable and falls within the definition of personal data.

Profiling Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work or studies, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Restriction of processing The marking of stored personal data with the aim of limiting their processing in the future.

Records of Processing Activities Detailed records of the personal data processing activities that a Data Controller or Processor is required to maintain and make available under the GDPR.

Supervisory authority An independent public authority established by the UK or another state to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of noncompliance. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

10. FURTHER HELP AND ADVICE

For further information and advice about this policy and any aspect of information security contact:

Kindi Education
Telephone: (+44) 121 6477 088
Email: info@kindieducation.com