Data Protection Policy

Owner: Group Service and Compliance Manager

Contents:

Classification: Internal

Data Protection Policy v1.2
April 2023

Document Control

Document History

Date	Version	Summary of Changes
14/05/2018	1.0	New Policy
15/08/2022	1.1	Annual Review
25/04/2023	1.2	Updated to latest group template and minor amendments

Approvals: This document requires approval from the Group Service and Compliance Manager

Name	Title	Date of Approval
Neil Cunningham	Group CEO	V1.0 22/05/2018
Nigel Ward	Group CFO	V1.0 22/05/2018
Emma Willis	Data Protection and Legal Compliance Manager	V1.0 22/05/2018
Lisa Eccleston	Senior Compliance Officer	V1.1 15/08/2022
George Woods	Group Service and Compliance Manager	V1.2 25/04/2023

Distribution: This document will be distributed via our internal intranet.

Frequency of review required: 1 year, and on an ad hoc basis

Data Protection Policy v1.2
April 2023

1 Introduction

The Kindertons Group is committed to complying with the law and regulations in all our activities, including applicable Data Protection Laws.

This policy, and the associated policies, set out the expected behaviours of Kindertons employees and contractors in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data held within the business.

Any references to 'Kindertons', 'we', 'our' and 'us' refers to all subsidiaries in The Kindertons Group.

2 Scope and Purpose

Personal Data is any information (including opinions and intentions) which relates to an identified or 'Identifiable Natural Person'. Personal Data is subject to certain legal safeguards and other regulations which impose restrictions on how organisations may process Personal Data. We are responsible for ensuring compliance with the data protection requirements outlined in this policy and the associated documents.

The Information Commissioner's Office (ICO) is responsible for upholding information rights in the public interest and enforcing the requirements of UK Data Protection Laws.

Kindertons is a Data Controller in respect of our customers and employee's data. In some circumstances, we may also be a joint Data Controller or Data Processor. The specific objective of this policy and associated policies is to ensure that all employees understand the requirements to comply with Data Protection Laws in relation to data held on customers, employees and contractors.

This policy applies to all processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy does not contain an exhaustive set of requirements. Employees should remember to comply with the spirit of the policy. The policy is subject to continuous review and new pages and/ or amendments may be issued from time to time. It is the responsibility of the individual to ensure they have access to the current version at all times.

If an employee or any associated person does not understand how the policy applies to them, or what action they should take they should speak to their line manager.

The scope of this policy will apply where a Data Subject's Personal Data is processed:

- In the context of our business activities
- For the provision or offer of services to individuals

Furthermore, the policy applies to all employees, contractors or third parties who may handle data on behalf of Kindertons. We will ensure that all Third Parties engaged to Process Personal Data on our behalf are aware of and comply with this policy.

3 Definitions

Personal Data	Any information (including opinions and intentions) which relates to an identified or identifiable natural person.
Identifiable natural person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as name, and 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 natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Subject	The identified or identifiable natural person to which the data refers.
Process, processed, processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulations – in the UK this is the ICO.
Data Processors	A natural or legal Person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Profiling	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an identifiable natural person. In particular to analyse or predict certain aspects concerning that natural person's performance at work economic situations, health, personal preferences, interests, reliability behaviour, location or movement.
Personal Data Breach	A breach of security leading to the accidental or unlawful; destruction, loss, alteration, unauthorised disclosure of, of access to, Personal Data transmitted, stored or otherwise Processed.
Encryption	The process of converting information or data into code, to prevent unauthorised access.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a key that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
GDPR	The General Data Protection Regulation

4 Roles and Responsibilities

All employees, including contractors and third parties who process data on behalf our behalf are responsible for complying with the requirements of this policy.

The Group Compliance Team are responsible for maintaining the policy, ensuring compliance with any Data Subject requests and ensuring incidents are reviewed and managed accordingly.

All Department Heads are responsible for ensuring that documented procedures are in place to comply with the requirements of this policy.

5 Policy

5.1 Data Protection Principles

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means we must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means we must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation
Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means we must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy
Personal Data shall be accurate and kept up to date. This means we must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation
Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means we must, wherever possible, store Personal Data in a way that limits or prevents identification of Data Subjects

Principle 6: Integrity & Confidentiality
Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. We must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Accountability
The Data Controller shall be responsible for, and be able to demonstrate compliance. This means we must be able to demonstrate that the six Data Protection Principles outlines above are met for all Personal Data for which it is responsible. We will do this through having policies and processes in place to ensure that personal data is held securely and is only processed in line with the relevant legislation.

5.2 Data Collection and Processing

Data Source
We will receive personal data in a variety of ways. We will collect data ourselves via telephone, email and our portal. We will also receive personal data from our sources and referrers. However data is received or collected, we will ensure that the data subject receives an appropriate privacy notice.

5.3 Data Subject Notification/External Privacy Notices

Kindertons will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data. We will do this through our Privacy Notice. The most up to date version of our Privacy Notice can be found on our website.

5.4 Data Use

Data Processing
Kindertons use the Personal Data for the following broad purposes:

- To provide claims, insurance and legal services to our customers
- To comply with employment law and other legal obligations

The use of the Data Subject's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Kindertons will process Personal Data in accordance with all applicable laws and applicable contractual obligations. We will only process Personal Data where one of the following conditions are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- The processing is in accordance with the legitimate "interests" condition

5.5 Special Categories of Data

Kindertons will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject
- The Processing is necessary for the establishment, exercise or defence of legal claims
- The Processing is specifically authorised as required by law
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health

5.6 Data Quality

Kindertons employees will ensure that the personal data they collect and process is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject by:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification
- Following the Group Data Retention Policy

5.7 Digital Marketing

We may send promotional or direct marketing material to customers through digital channels such as mobile phones, email where their details have been obtained through the provision of our services to them and where the materials relate to a similar service which may be of benefit to them. We will inform the Data Subject that they have the right to object to direct marketing at any stage. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision.

5.8 Data Retention

To ensure fair Processing, Personal Data will not be retained by Kindertons for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. Further details are set out in our Group Data Retention Policy.

5.9 Data Security

We will adopt physical, technical and organisational measures to ensure that security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access of Processing, and other risks to which it may be exposed by virtue of human action of the physical or natural environment.

Data security and protection measures are set out in our Information Security Policy.

5.10 Data Subject Requests

We have established procedures to enable and facilitate the exercise of Data Subject Rights relating to:

- Information access
- Objection to Processing
- Objection to automated decision-making and profiling
- Restriction of Processing

- Data portability
- Data rectification
- Data erasure

If a Data Subject makes a request relating to any of the rights listed above we will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. The decision whether or not to charge a fee will be taken by the Group Compliance Team.

A response to any request will be provided within 30 days of the receipt of the request from the Data Subject. Appropriate verification checks will be carried out to confirm that the individual requesting the data is the Data Subject or their authorised legal representative. Data Subjects have the right to require us to correct or supplement misleading, outdated or incomplete Personal Data.

Further information on responding to Data Subject requests can be obtained from the Group Compliance Team.

5.11 Law Enforcement Requests & Disclosures

In certain circumstances we will be required share Personal Data without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the Order of a court or by any rule of law

If we process personal data for one of these purposes then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any employee receives a request from a Court or any regulatory or law enforcement authority for information relating to a customer this must be immediately brought to the attention of the Group Compliance Team by emailing privacy@kindertons.co.uk

5.12 Transfers to Third Parties

We will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, we will first identity if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller we will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred. Where the Third Party is deemed to be a Data Processor we will enter into an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with our instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

5.13 Complaint Handling

Data Subjects with a complaint about the Processing of their Personal Data should direct their complaint for the attention of the Customer Experience Team by emailing customerexperienceteam@kindertons.co.uk. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Customer Experience Team will inform the Data Subject of the progress and the outcome of the complaint once investigations are concluded. Kindertons aims to resolve where possible all complaints within 56 days. If the

issue cannot be resolved through consultation between the Data Subject and the Customer Experience Team, then the Data Subject may at their option, seek redress through mediation, binding arbitration, litigation or via complaint ICO. Any employee who receives a complaint should forward it to the Customer Experience Team [customerexperienceteam@kindertons.co.uk] immediately.

5.14 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Group Compliance Team by emailing privacy@kindertons.co.uk, if the breach relates to an information security issue then the notification should be sent to security@kindertons.co.uk

5.15 Data Protection By Design and Default

Article 25 of the GDPR states:

" (1)….the controller shall, both at the time of the determination of the means of processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as Pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

To ensure that we identify all Data Protection requirements when designing new systems or processes and/or when reviewing or expanding existing systems or processes, a Data Protection Impact Assessment (DPIA) will be conducted.

6 Training

All employees will have their responsibilities under this policy outlined to them as part of their induction training. All employees will complete an annual refresher of this training. We will provide further training and guidance if there are any updates made to this policy and/or the associated policies and procedures.

7 Monitoring Compliance

As a minimum the following will be monitored to ensure compliance with this policy: -

- An annual Data Protection Compliance Audit which will, at the minimum assess:
  - Compliance with policy in relation to the protection of personal data, including;
    - The assignment of responsibilities.
    - Raising awareness.
    - Training of employees.
  - The effectiveness of Data Protection related operational practices, including;
    - Data subject's rights.
    - Personal Data transfers.
    - Personal Data incident management.
    - Personal Data complaints handling.
  - The level of understanding of Data Protection policies and privacy notices.
  - The currency of Data Protection policies and privacy notices.

- o The accuracy of Personal Data being stored.
- o The conformity of Data Processor activities.
- o The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

Key business stakeholders will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Group Compliance Team**.**

8 Review

This policy is owned by the Group Compliance Team and will be reviewed at least annually. We will provide information and/or training on any changes we make.

9 Related Documents

- Group Data Retention Policy
- Group Privacy Notice