Data Protection Policy

Located on SharePoint: IMS: Procedures

Controlled Document: 000

Kao Data Campus Locations

- London Road, Harlow, CM17 9NA
- Galvin Road, Slough, SL1 4AN
- Rowdell Road, Northolt, UB5 6AG

Document Change History

Version No.	Date Issued	Update Details	Issued by	Approved by
V2.0	30/05/2022	Original Document	Gary Kilmister	Joanna Breen
V2.1	30/05/2022	Draft revision and updates	Gary Kilmister	Joanna Breen
V2.2	15/06/2022	Standardise new format and structure, revised some updates	Gary Kilmister	Paul Finch / Lee Myall
V3.0	24/06/2022	Published version – sign off	Gary Kilmister	Gary Kilmister
V3.1	25/06/2023	Periodic Review of document – no significant changes	Gary Kilmister	Gary Kilmister
V3.2	10/07/2023	Minor amendment made to footer to remove reference to ISO standards	Katie Harper	Gary Kilmister
V3.3	27/07/2023	Final version for sign off and approval	Gary Kilmister	Paul Finch / Lee Myall
V4.0	28/07/2023	Published Version – signed off	Gary Kilmister	Gary Kilmister

Distribution List

Copy Number	Job Title / Purpose	Location
000	Master	SharePoint

Contents

KAO DATA

1. Purpose

Kao Data as an organisation is committed in being transparent about how it collects and uses the personal data of its employees. This policy sets out the company's commitment to data protection, and individual rights and obligations in relation to personal data in accordance with the EU General Data Protection Regulation 2018 (GDPR) and the Data Protection Act 2018 (DPA).

2. Applicability

This policy applies to the personal data of job applicants, employees, agency workers, contractors, volunteers, interns, apprentices, consultants, and former employees, referred to as HR-related personal data.

This policy does not apply to the personal data of clients or other personal data processed for business purposes.

This policy is non-contractual and may be amended anytime at the Company's absolute discretion.

3. Definitions

"**Personal data**" is any information that relates to a living individual who can be identified from that information and includes any expression of opinion about the individual and any indication of intention in respect of that individual. It doesn't include data that has been anonymised.

Personal data may be provided to us by you, but may also be provided to us by third parties (such as former employers), or may be created during the employment relationship (e.g. appraisal records) or on its termination (e.g. references provided to prospective employers).

"**Special categories of personal data**" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Kao Data may collect information from you relating to some of the above categories but will usually do so in an anonymised way, for example to monitor the effectiveness of our equal opportunities policy. Where this is the case, it will not be considered to be personal data. However, where the data has not been anonymised or pseudo anonymised, this will clearly be special category of data and will be treated as such.

"**Criminal records data**" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

"Processing"

is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

4. Data Protection Principles

Kao Data processes HR-related personal data in accordance with the six data protection principles, which sets out that all personal data will and shall be:

- processed lawfully, fairly and in a transparent manner.
- collected and processed only for specified, explicit and legitimate purposes.
- adequate, relevant, and limited to what is necessary for the purposes of processing.
- accurate and in date data – Any inaccurate personal data will be rectified or deleted without delay.
- kept only for the period necessary for processing.
- processed in a way that ensure appropriate security and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The company will tell individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the company relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of the individual(s).

The company will update its HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in either hard copy, electronic format, or both), on our HR management systems, other IT systems (including the company's email system), security records and systems, time keeping records, telephone recording or monitoring systems and the company reserves the right to use CCTV as applicable.
The company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

5. Lawful Processing

In line with the data protection principles, Kao Data will only process your personal data and special category data for the reason notified to you in accordance with our obligations. Under the DPA we must have a specified lawful basis for processing your personal data.

Kao Data processes personal data where necessary to manage employment relationship and the main lawful basis for processing your data is:

- to comply with our legal obligations (e.g. paying your tax)
- to perform your contract with us (e.g. pay you according to the rate agreed)
- because it is necessary for our legitimate interests (e.g. to ensure that we can succession plan)

Where one of these reasons applies, we may process your data without your consent. You may choose not to give us certain data, but you should be aware that this may prevent us complying with our legal obligations and this may in turn affect your employment.

Where the company processes special category data, we will only do so where one of the lawful reasons set out above applies and where either:

- you have given your explicit consent
- processing is necessary under employment law
- processing is necessary to protect you, or another person's vital interest and you are incapable of giving consent
- you have made the data public
- processing is necessary for occupational medical reasons or for the assessment of your working capacity

Where we plan to process special category data relating to you, we will explain this and set out the reasons at the time.

6. Individual Rights

Individuals have a number of other rights in relation to their personal data. They:

- can rectify inaccurate data by contacting their line manager
- stop processing or erase data that is no longer necessary for the purposes of processing
- may ask the company to stop processing or erase data if the individual's interests override the company's legitimate grounds for processing this data (where the company relies on its legitimate interests as a reason for processing data)
- may ask the company to stop processing or erase data if processing is unlawful

- may ask the company to stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the company's legitimate grounds for processing this data
- will be notified if there is a data security breach involving their data that may affect them
- have the right not to consent, or to later withdraw your consent to processing where we were relying on consent as the lawful reason to process personal data

To ask the company to take any of these steps, the individual should send the request to their line manager.

7. Subject Access Requests

Individuals have the right to review the information that Kao Data holds about them making a subject access request. Subject access requests should be in writing to your line manager.

The company will normally respond to a request within a period of **one month** from the date it is received. If your request is complex, then the company may respond within three months of the date the request is received. The company will notify you in writing within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. Alternatively, the company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the company has already responded. If you submit a request that is unfounded or excessive, the company will notify you that this is the case and whether it will respond to it.

8. Data Security

Kao Data takes the security of HR-related personal data seriously. The company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

9. Individual Responsibilities

Individuals are responsible for helping the company keep their personal data up to date. Individuals should let the company know if data provided to the company has changed, for example if they move to a new house or change bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of your employment, contract, volunteer period, internship, or apprenticeship. Where this is the case, Kao Data relies on them to help meet its data protection obligations to staff and to customers and clients. You must therefore familiarise yourself with this policy, including the data protection principles and comply with them.

If you have access to personal data, you are required:

- to access only data that you have authority to access and only for authorised purposes
- not to disclose data (e.g., through social media or emails) except to individuals (whether inside or outside the organisation) who have appropriate authorisation
- to keep data secure – whether on paper or electronically. You must use strong passwords and always lock your PC/device when not in use. You must keep personal data in locked cabinets
- to securely destroy any copies of personal data you create
- not to remove personal data, or devices containing or that can be used to access personal data, from the company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; printed copies must not be removed from the company premises without specific authorisation
- to protect any personal data contained in portable devices (e.g., memory sticks, CDs, DVDs, mobile phones, laptops, tablets, etc. – this list is not exhaustive). Loss of any portable device containing personal data must

be immediately reported to your line manager. Failure to report this constitutes a disciplinary offence and could lead to summary dismissal for gross misconduct.

- not to store personal data on local drives or on personal devices that are used for work purposes.
- to report data breaches of which you become aware to your line manager immediately. Failure to report any data breach could constitute a disciplinary offence and could lead to summary dismissal for gross misconduct.

10. Monitoring

Kao Data may monitor your use of the workplace computer systems (including emails and use of internet on workplace computers or other devices) to protect other employees and because of duties owed to suppliers and clients.

If any monitoring is being considered you will be advised of this and given all the relevant information, including the lawful basis for processing the data, at the time such monitoring is put in place. Where processing would result in a high risk to individual's rights and freedoms, the company will carry out a Privacy Impact Assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Covert monitoring will only take place exceptionally and where the Privacy Impact Assessment has established that there is no less intrusive way to gather the information.

11. Data Handled By Third Parties

Where Kao Data engages with third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

12. Privacy Notices

Whenever Kao Data collects information from you, is provided with information about you or are planning to pass information onto a third party, we will provide you with a privacy notice giving clear information about how and why your data is being used, where it comes from and where it goes.

This section gives an overview of the data we usually collect and use about you during your relationship with us. As your employer we need to process your personal data during your recruitment, your employment with us and following the termination of your employment.

We will use the data listed below to check whether to employ you, check you have the right to work in the UK, decide what salary and other terms to offer you and then administer the ongoing contract between us including, for example, managing your performance and conduct, making reasonable adjustments if you have a disability, paying you and deducting tax and national insurance.

- Your name and date of birth
- Your address, telephone number and personal email address
- Your ID documents and information about immigration status
- Your NI number and details of your tax status
- Information about your previous employment history
- Your qualifications and professional memberships
- Your job title and place of work
- Information about your contract with us including your start date, working hours and salary and benefits information
- Your gender, marital status, and details of any dependants
- Contact details of your emergency contact
- Information about your performance including appraisal records
- Details of any training received
- Details of any grievances raised or in which you were involved

- Disciplinary records including investigations and warnings
- Attendance records, including absence and sickness information
- Images of you from our on-site CCTV systems
- Records of any correspondence between you and the organisation about your employment including, for example, letters confirming any changes to your contract of employment

13. Retention Periods

If Kao Data collects your personal information, the length of time we retain it is determined by several factors including the purpose for which we use that information and our obligations under other laws.

We may need your personal information to establish, bring or defend legal claims. For this purpose, we will always retain your personal information for 6 years after the end of your employment with us. The only exceptions to this are where:

- the law requires us to hold your personal information for a longer period, or delete it sooner
- you exercise your right to have the information erased (where it applies) and we do not need to hold it in connection with any of the reasons permitted or required under the law
- we bring or defend a legal claim or other proceedings during the period we retain your personal information, in which case we will retain your personal information until those proceedings have concluded and no further appeals are possible
- in limited cases, existing or future law or a court or regulator requires us to keep your personal information for a longer or shorter period.

14. Training

Kao Data will provide training to all individuals about their data protection responsibilities as part of the induction process. Adherence to Data Protection is a fundamental part of the Induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

15. Breaches of This Policy

Failing to observe the requirement of this policy may amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure.

Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

16. Sign off

Signed

DocuSigned by:
A8EE0FF33B86457...

Lee Myall
Chief Executive Officer, Kao Data
Published: July 2023

Signed

DocuSigned by:
Paul Finch
F3849356F76B49B...

Paul Finch
Chief Operating Officer, Kao Data
Published: July 2023