



Information Classification and Handling Policy



The copyright of this document is vested in Kao Data. This document may only be reproduced in whole or in part, or stored in a retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying or otherwise, with the prior permission of Kao Data

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

Information Classification and Handling Policy

Document Change History

Version No.	Date Issued	Update Details	Issued by	Approved by
V4.0	24/03/2021	Published version.	Caroline Curtis	Jashan Babra
V4.1	18/04/2022	Reformatting of document and updating for re-publication – Version history enabled	Gary Kilmister	Gary Kilmister
V4.2	12/08/2022	Final Document for publishing, sent for approval and sign off (added sign off section)	Gary Kilmister	Paul Finch Lee Myall
V5.0	15/08/2022	Published and Re-issued	Gary Kilmister	Gary Kilmister
V5.1	10/07/2023	Minor amendment made to footer to remove reference to ISO standards. Amended Moderate to Medium to align with the rest of the document.	Katie Harper	Gary Kilmister
V5.2	22/08/2023	Periodic review of document and update contents for consistency across the document	Gary Kilmister	Gary Kilmister
V5.3	22/08/2023	Final Document for publishing, sent for approval and sign off (added sign off section)	Gary Kilmister	Paul Finch Lee Myall
V6.0	23/08/2023	Published and Re-issued	Gary Kilmister	Gary Kilmister

Distribution List

Copy Number	Job Title	Location
000	Master	SharePoint

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 2 of 13

Information Classification and Handling Policy

Contents

1	Purpose	4
2	Applicability	4
3	Classification of Information	4
3.1	Impact Levels	4
3.2	Assessment	4
3.3	Company Information Classifications	4
3.3.1	Public	4
3.3.2	Internal	4
3.3.3	Confidential	4
3.3.4	Highly Sensitive (Restricted)	4
4	Pre-classified Information	5
4.1.1	Internal (LOW Impact)	5
4.1.2	Confidential (MEDIUM Impact)	5
4.1.3	Highly Sensitive (Restricted) (HIGH Impact)	5
5	Labelling requirements	5
6	Handling requirements	5
7	Maintenance of Information Classifications	7
8	Handling of Information Media	8
9	Equipment Re-use	8
10	Disposal of Media (End of life)	9

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 3 of 13

Information Classification and Handling Policy

1 Purpose

Kao Data has defined the minimum requirements to ensure that information is handled and protected appropriately. As a minimum, all Company, Client, and Personal data must conform to the controls described below.

2 Applicability

This policy is applicable to all stakeholders, employees and contractors and third-party suppliers working for or on behalf of Kao Data.

All employees and contractors of Kao Data, whether on a permanent or temporary basis, are subject to this policy. At the same time, individuals may be personally liable for any conduct and/or action(s) that may be unlawful or illegal.

Any breach of this policy by an employee of Kao Data may result in disciplinary procedures being implemented and may lead to dismissal for gross misconduct. Any breach of this policy by a contractor may lead to the termination of any such engagement or arrangement.

3 Classification of Information

Information held should be assessed and classified according to the following sections.

3.1 Impact Levels

There are several levels of potential impact on the company or individuals should there be a breach of information security (e.g., a loss of confidentiality, integrity, or availability of information):

There is **NO** impact if the information is in or can be put into the public domain with no concerns, can be unreliable or inaccurate with no concerns, and if there are no concerns if it is lost or unavailable.

The potential impact is **LOW** if:

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on the company's operations, assets, or on individuals.

The potential impact is **MEDIUM** if:

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on the company's operations, assets, or on individuals.

The potential impact is **HIGH** if:

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on the company's operations, assets, or on individuals.

3.2 Assessment

The information owner should assess their information against each security objective (confidentiality, integrity, and availability) and determine the potential impact. The information should then be classified based on the highest potential impact level for that information.

3.3 Company Information Classifications

Information should be designated one of the following company classifications and handled accordingly.

3.3.1 Public

If there is NO potential impact in terms of unauthorised disclosure, unauthorised modification, then the data set should be classified as **PUBLIC**.

3.3.2 Internal

If the potential impact in terms of unauthorised disclosure, unauthorised modification, or loss of data is identified as 'LOW', then the data set should be classified as **INTERNAL**.

3.3.3 Confidential

If the potential impact in terms of unauthorised disclosure, unauthorised modification, or loss of data is identified as 'MEDIUM', then the data set should be classified as **CONFIDENTIAL**.

3.3.4 Highly Sensitive (Restricted)

If the potential impact in terms of unauthorised disclosure, unauthorised modification, or loss of data is identified as 'HIGH', then the data set should be classified as **HIGHLY SENSITIVE (RESTRICTED)**.

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 4 of 13

Information Classification and Handling Policy

4 Pre-classified Information

The information owner should decide as to the most appropriate category for their information; however, the following items have already been categorised:

4.1.1 Internal (LOW Impact)

Policies, Standard Operating Procedures

4.1.2 Confidential (MEDIUM Impact)

HR data, supplier contracts, operations reports, accounting records

4.1.3 Highly Sensitive (Restricted) (HIGH Impact)

Corporate such as Strategy, Planning, Investment and Funding; Customer Negotiation and Contracts

5 Labelling requirements

HIGHLY SENSITIVE and **CONFIDENTIAL** information should be clearly identifiable with appropriate markings if there is any possibility its categorisation could be mistaken.

Other information is not necessarily marked, and unless it is completely clear that the information is **PUBLIC**, all other information should be handled according to **INTERNAL**.

6 Handling requirements

Depending on the Classification of the information the following requirements apply.

NOTE: These are a company **MINIMUM** and additional measures can be applied on a case-by-case basis by information owners and/or managers where this is deemed appropriate.

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 5 of 13

Information Classification and Handling Policy

CLASSIFICATION	STORAGE	TRANSIT (EMAIL AND PHYSICAL)	SHARING	DISPOSAL
PUBLIC	Any (as appropriate)	Can be distributed freely	Can be shared freely	Can be disposed of freely
INTERNAL	<ul style="list-style-type: none"> Approved Cloud based and Company systems and applications (list here e.g., SharePoint) Clear Desk & Clear Screen Policies apply 	Approved systems and applications can be used with no additional controls	These types of documents can be shared within the company and with interested parties	Electronically via the software's deletion facility NB: It is good practice to shred physical copies (though not mandatory)
CONFIDENTIAL	<ul style="list-style-type: none"> Approved Cloud based and Company systems and applications (list here e.g., SharePoint, Office365, NetSuite, MoorePay, Peninsular HR) Access to applications and shared folders to be restricted based on role If stored in an insecure location (e.g., USB stick, removable drive or laptop) it must be encrypted (by default USB, Removable drive are denied via policy – so if used exception must be approved by SMT / Compliance) If hard copy, then must be stored in a locked drawer or filing cabinet when unattended Clear Desk & Clear Screen Policies apply 	<ul style="list-style-type: none"> The information must be encrypted in transit and encryption keys exchanged via a separate channel Documents transferred over e-mail, should be password protected to provide levels of protection. If posted, then must be by Recorded / Special Delivery 	These types of documents can be shared within the company and with relevant interested parties	Electronically via the software's deletion facility Shred physical copies

Information Classification and Handling Policy

CLASSIFICATION	STORAGE	TRANSIT (EMAIL AND PHYSICAL)	SHARING	DISPOSAL
HIGHLY SENSITIVE (RESTRICTED)	<ul style="list-style-type: none"> Approved Cloud based and Company systems and applications (list here e.g., SharePoint, Office365, NetSuite, MoorePay, Peninsular HR) Access to applications and shared folders to be restricted based on role If stored in an insecure location (e.g., USB stick, removable drive or laptop) it must be encrypted (by default USB, Removable drive are denied via policy – so if used exception must be approved by SMT / Compliance) If hard copy, then must be stored in a locked drawer or filing cabinet when unattended Clear Desk & Clear Screen Policies apply 	<ul style="list-style-type: none"> The information must be encrypted in transit and encryption keys exchanged via a separate channel Documents transferred over e-mail, should be password protected to provide levels of protection. If posted, then must be by Recorded / Special Delivery 	This type of information can only be shared on a NEED TO KNOW basis	<p>Electronically via the software's deletion facility</p> <p>Shredded or certificated disposal only (electronic and physical media)</p>
ALL EMPLOYEES	<ul style="list-style-type: none"> Clear Desk and Screen Policy 	Standard company policy, no internal, confidential or highly sensitive information is to be left on desk, if printed documentation is required, then this is locked away. Company policy, when away from your desk, your screen MUST be locked		

7 Maintenance of Information Classifications

Once the information classification scheme and mappings have been completed, they need to be managed to stay current with the business and technical environments.

The following steps outline the review process.

- The information classification mappings and protective controls are reviewed on a regular basis (at least annually, depending on the rate of change within the business and technical environments).
- Information classifications will be reviewed as part of each new product/service project.

Awareness training will be provided to all staff once the annual review of the information classification has taken place should there have been any amendments.

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 7 of 13

Information Classification and Handling Policy

8 Handling of Information Media

To protect information, the information media must be safeguarded against disclosure, theft, or damage. Proper media labelling, storage, transport, and disposal are risk mitigation controls.

The following sections describe how to handle different media types and events in the media lifecycle. When in doubt about the information stored on media, label, log, and securely store media.

- Regardless of method, the handling, processing, transmission and/or storage of company information should be affected through means that limit the potential for unauthorised disclosure.
- Media should be labelled to ensure information can be logged, tracked and effectively protected.
- Employees whilst travelling or working away from the office should ensure that company information is adequately safeguarded from unauthorised access. This applies regardless of whether the information is in paper form, DVD, USB stick, removable drive or other electronic readable media.
- Employees transmitting sensitive company information via non-secure fax must ensure that an authorized recipient is ready to receive it at the other end.
- Company information may be sent via Royal Mail or a commercial delivery service, e.g., DPD. Where possible mail must be packaged in a way that does not disclose its contents.
- During non-office hours, company information and removable electronic media must be secured within a locked office or secured in a locked container.
- Custodians of all personnel information must ensure that it is secured when not in use.

9 Equipment Re-use

The following procedures should be followed when re-using equipment.

- Before re-use, back up all required material from hard disks, DVDs, USB sticks and other media.
- The IT Manager or the designated person responsible for IT, will use appropriate software to remove all data, wipe the media and prepare it for re-use (Secure Erase report/certificate will be stored within IMS (where applicable)).
- Once a device has all data removed, consideration should be given to the re-use of that device. Considerations will include condition/age of device, previous use, compatibility and availability of support (including firmware updates).

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 8 of 13

Information Classification and Handling Policy

10 Disposal of Media (End of life)





The following procedures should be followed when disposing of records and equipment.

- Before disposal of electronic media, back up all required material from hard disks, DVDs, USB sticks, etc.
- Any device that can store data should be passed to the IT Manager. The IT Manager will be responsible for storing media awaiting disposal in a secure location.
- The IT Manager will remove all data from disks, USB sticks, etc, to ensure no information can be extracted and then dispose of the media using an approved disposal company (where onsite destruction is not to be carried out).
- With regards to storage devices, a secure erase will be completed and a certificate as evidence that this has been carried out (where applicable) will be stored within IMS.
- All electronic equipment must be disposed of in accordance with UK WEEE regulations and the Waste and Recycling Management Guide.
- Paper media should be shredded where required by its classification and recycled where possible.
- Access Cards will be secure shredded as part of leaver process, or if incorrect pass as likes of some facility passes have photos, or other personal information on them.

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 9 of 13

Information Classification and Handling Policy

1. ASSESS THE INFORMATION CONTENT USING THE FLOW CHART BELOW TO PROVIDE CLASSIFICATION

Security Objectives	WHAT IS THE POTENTIAL IMPACT?			
	NONE	LOW	MEDIUM	HIGH
Confidentiality What could happen if it was disclosed without authorisation?	No adverse effect on company, if information is in or can be put into the public domain with no concerns, can be unreliable or inaccurate with no concerns, and if there are no concerns if it is lost or unavailable. 	Limited adverse effect on the company operations, assets, or on individuals. 	Serious adverse effect on the company's operations, assets, or on individuals. 	Severe or catastrophic adverse effect on the company's operations, assets, or on individuals. 
Integrity - What could happen if/when modified or destroyed without authorisation?				
Availability What happens if information is disrupted or accessed without authorisation?				
WHAT SHOULD IT BE CLASSIFIED?	PUBLIC No potential impact in terms of unauthorised disclosure, unauthorised modification	INTERNAL Discretion of the custodian Low risk of embarrassment or reputational harm to the company.	CONFIDENTIAL Legal, regulatory or contractual obligation to protect the information with this classification. Harm to the reputation of the company, or may have short-term financial impact.	HIGHLY SENSITIVE (RESTRICTED) Required by law or regulatory instrument. Strictly limited distribution within and outside the Company. Disclosure would cause exceptional or long-term damage to reputation or risk to those whose information is disclosed, or may have serious or long-term negative financial impact on the Company.

Information Classification and Handling Policy

2. ONCE CLASSIFIED ENSURE YOU ARE STORING, MARKING AND DISPOSING OF CORRECTLY			
<p>PUBLIC <i>Public web page, press releases, event details and advertisements, some policies, certification, memberships</i></p>	<p>INTERNAL <i>HR data, supplier contracts, operations reports, accounting records, policies, procedures, blank templates and guidance</i></p>	<p>CONFIDENTIAL <i>Quotes, proposals, HR data, supplier contracts, operations reports, accounting records, customer requested (NDA), Customer Negotiation and Contracts</i></p>	<p>HIGHLY SENSITIVE (RESTRICTED) <i>Bid and proposal documents flagged as highly sensitive; sensitive financial information; health record relating to individuals; Board or confidential reports; Corporate such as Strategy, Planning, Investment and Funding; Customer Negotiation and Contracts flagged as highly sensitive;</i></p>
HOW SHOULD I STORE IT?			
<p>As appropriate</p>	<p>Approved Cloud based and Company systems and applications (e.g., SharePoint). Clear Desk & Clear Screen Policies apply</p>	<p>Approved Cloud based and Company systems and applications (e.g., SharePoint, Office365, NetSuite, MoorePay, Peninsular HR) Access to applications and shared folders to be restricted based on function, role and responsibilities. If stored in an insecure location (e.g., USB stick, removable drive or laptop) it must be encrypted (by default USB, Removable drive are denied via policy – so if used exception must be approved by SMT / Compliance If hard copy, then must be stored in a locked drawer or filing cabinet when unattended Clear Desk & Clear Screen Policies apply</p>	<p>Approved Cloud based and Company systems and applications (e.g., SharePoint, Office365, NetSuite, MoorePay, Peninsular HR) Access to applications and shared folders to be restricted based on function, role and responsibilities. If stored in an insecure location (e.g., USB stick, removable drive or laptop) it must be encrypted (by default USB, Removable drive are denied via policy – so if used exception must be approved by SMT / Compliance If hard copy, then must be stored in a locked drawer or filing cabinet when unattended Clear Desk & Clear Screen Policies apply</p>

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance	IN HARD COPY FORMAT	Page No.	Page 11 of 13



Information Classification and Handling Policy

WHAT SHOULD IT BE MARKED, HOW CAN IT BE SENT & WHO IS RESPONSIBLE?			
<p>No marking required Can be distributed freely Can be shared freely</p> <p>Unless it is completely clear that the information is PUBLIC, all other information should be handled according to INTERNAL.</p>	<p>'INTERNAL' marking on bottom of page may be used but is not mandatory. These types of documents can be freely distributed internally or to contractors and third parties who have signed an appropriate nondisclosure agreement.</p>	<p>'CONFIDENTIAL' marking on bottom left of page if there is any possibility its categorisation could be mistaken. Transmit: The information must be encrypted in transit and encryption keys exchanged via a separate channel Documents transferred over e-mail, should be password protected to provide levels of protection. If posted, then must be by Recorded / Special Delivery</p>	<p>'HIGHLY SENSITIVE' marking on bottom left of page if there is any possibility its categorisation could be mistaken. Transmit: The information must be encrypted in transit and encryption keys exchanged via a separate channel. If faxed, then it needs to be collected from the fax machine by the receiver If posted, then must be by Special Delivery</p>
	<p>Transmit: Approved systems and applications can be used with no additional controls Share: These types of documents can be shared within the company and with relevant interested parties</p>	<p>Share: These types of documents can be shared within the company and with relevant interested parties</p>	<p>Share: This type of information can only be shared on a NEED-TO-KNOW basis</p>
PUBLIC	INTERNAL	CONFIDENTIAL	HIGHLY SENSITIVE (RESTRICTED)
HOW SHOULD IT BE DISPOSED?			
Can be disposed of freely.	Electronically via the software's deletion facility NB: It is good practice to shred physical copies (though not mandatory)	Electronically via normal deletion facilities. Paper copy via confidential shredding.	Electronically via the software's deletion facility Shredded or certificated disposal only (electronic and physical media)

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 12 of 13

Information Classification and Handling Policy



11 Changes to this Policy

We reserve the right to amend or modify this Policy without notice to you and if we do so we will post the changes on this page. It is your responsibility to check our Policy each time before you access our website for any changes.

12 Sign off

Signed

DocuSigned by:

A8EE0FF33B86457...

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

Signed

DocuSigned by:

F3849356F76B49B...

Paul Finch
Chief Operations Officer, Kao Data
Published: August 2023

Document Title:	Information Classification & Handling Policy	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	23/08/2023
Version Number:	V6		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 13 of 13