Data Protection & Document Retention Policy

Introduction

This Data and Document Retention Policy sets out how we, at Thalia Waste Management, classify and manage the collection, retention, protection and disposal of our data during our day-to-day business activities and provision of services.

We recognise the importance of data protection both in respect of our internal responsibilities but also in respect of our customers, partners, suppliers and each of their respective businesses.

Any breach of this policy will be taken seriously and may result in disciplinary action. In certain circumstances of the mishandling of data, the data protection laws applicable in the UK include provisions for criminal offences.

This policy does not form part of any employee's contract of employment with Thalia Waste Management.

Definitions and Principles

Definitions

Data includes data in physical media such as hard copy documents, contracts, notebooks, letters and invoices. Data is also contained in electronic media such as emails, electronic documents, audio and video recordings and CCTV recordings. Some data may be personal some may be non-personal. In this policy we refer to all this information and these records collectively as “data”.

Data Breaches Register is the register held by us showing instances where we have not or potentially have not complied with GDPR. It is maintained by the Data Governance Manager.

Data Controller means the person or organisation that determines the purpose and means of the processing of personal data. Each Thalia Waste Management entity is the data controller of all personal data used in its business for its own commercial purposes.

Data Processors include any person or organisation that processes personal information on the instruction of a data controller.

Data Subject Access Requests are requests by Data Subjects for data pursuant to GDPR. These are handled by the Data Governance Manager.

Data Subjects for the purpose of this policy means all living individuals for whom we hold personal data, for example staff, customers, suppliers, job applicants and need not be UK national or resident.

Data Users are those employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy and any data security work practices.

Information Governance Manager (IGM) is a person whose responsibilities are set out under Information Governance in this policy.

Personal Data means information relating to a living individual directly identifiable from the information or who can be indirectly identified from that information in combination with other information and includes all personal

information we process regardless of how that data is stored or whether it relates to past or present employees, job applicants, workers, agency workers, consultants or contractors, interns, apprentices, volunteers, customers, clients or supplier contacts, shareholders, website users or any other individual.

Sensitive Personal Data includes information about a persons ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data, data concerning health or sex life and sexual orientation, physical or mental health data, criminal convictions and/or alleged offences. Sensitive personal data must be processed under strict conditions, including the express permission of the person concerned.

Processing is any activity or operation that involves the use of personal data, whether by retrieving, amending, using, disclosing, organising, consultation, recording, erasing or destroying.

This policy covers data that is held by other third parties on our behalf, for example, data held for us by cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.

GDPR Key Principles

All those processing personal data, whether electronically or in paper format, must comply with the applicable data protection laws. The seven key principles as set out within the General Data Protection Regulation (GDPR) and which lie at the heart of our approach are:

- personal data will be processed lawfully, fairly and in a transparent manner in relation to individuals;
- personal data will be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- personal data minimisation – the data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- personal data will be accurate and, where necessary, kept up to date and any inaccurate data be erased or rectified without delay;
- personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (storage limitation);
- integrity and confidentiality (security) is maintained, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- the Data Controller shall be responsible for, and be able to demonstrate compliance showing accountability.

These are the 7 Data Protection Principles with which we shall comply.

Personal data will not be transferred to another country without appropriate safeguards being in place and/or the transfer falls within the exceptions provided for in GDPR and/or the EU has made an adequacy decision.

Policy ownership and review

This policy is owned by our General Counsel. It will be implemented by the Data Governance Manager, reviewed annually and amended from time to time.

Roles and responsibilities

Information Governance

We have designated a Data Governance Manager (DGM) who is responsible for:

- managing Data Subject Access Requests from start to finish (sourcing, collating, analysing, redacting);
- maintaining and updating the Data Breaches Register with both minor breaches and those reportable to the ICO (complete data breach form and reply to any correspondence from the ICO);
- managing the GDPR Inbox;
- maintaining the Record of Processing;
- helping Account Directors and functional heads implement the data management programme and related best practices;
- planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- providing guidance, training, monitoring and updating in relation to this policy.

The DGM is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. The DGM works with the rest of the Data Governance Team on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

We have not designated a Data Protection Officer because of the nature of the personal data that we retain. This decision will be reviewed from time to time by the DGM and referred to our General Counsel if required.

Responsibility of all employees

All employees are responsible for helping us keep their personal information up to date.

You should update your personal information as soon as possible if the personal information you have provided to us changes, for example if you move house or change details of the bank or building society account to which you are paid. Should you need further assistance, please contact the HR Helpdesk.

You may have access to the personal information of other members of staff, suppliers and customers or clients of ours, that we are responsible for, in the course of your employment or engagement or otherwise. If so, we expect you to help meet our data protection obligations to those individuals. If you do have such access to personal information, you must:

- only access or obtain the personal information to which you have a job-related need and authority to access or obtain, and only for authorised and lawful purposes;
- only allow other Thalia Waste Management staff to access or obtain personal information if they have a job related need to access that information, appropriate authorisation and a lawful reason for

doing so;

- only allow individuals who are not Thalia Waste Management staff to access personal information if you have specific authority to do so from the DGM and suitable safeguards and contractual arrangements have been put in place (see paragraph 12, Information Security above, for more information);
- ensure that the personal information we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it;
- keep personal information secure (e.g. by complying with our rules on access to premises, computer access, password protection, secure file storage, destruction and other precautions;
- not remove personal information, or devices containing personal information (or which can be used to access it), from Thalia Waste Management's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device;
- not store personal information on local drives or on personal devices that are used for work (or other) purposes;
- comply with this Policy and our related policies and procedures; and
- not keep personal information in a form which enables the individual, that it relates to, to be identified for longer than needed for the legitimate business reason(s) for which we originally collected it, and comply with our Data Retention Policy and retention periods.

You should contact the Information Governance Team at legalservices@thalia.co.uk if you have any questions about this or are unclear about your responsibilities or if you are concerned or suspect that we have failed in our obligations under the relevant data protection laws or have failed to comply with this policy.

An example of a failure might include:

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information or criminal records information, without one of the conditions set out above being met;
- any data breach;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from our premises without appropriate security measures being in place;
- personal information being retained for longer than it is legitimately needed for; and
- any other breach of this Policy or any of our related policies or procedures, or any of the Data Protection Principles set out above.

Lawful Reasons for Processing Personal Information

In relation to any processing activity we shall, before the processing starts for the first time and then regularly while it continues:

- review the purposes of the particular processing activity, and identify the most appropriate lawful reason(s) for that processing, which may be one, or a combination of:
    - that the data subject has consented to the processing (this will only apply in limited circumstances);
    - that the processing is necessary for the performance of a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract;
    - that the processing is necessary for compliance with a legal obligation to which Thalia Waste Management is subject;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
    - that the processing is necessary for the purposes of legitimate interests of Thalia Waste Management or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject;
- (except where the processing is based on consent) satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the 7 Data Protection Principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant Privacy Notice(s) and provide a copy of this to the individual(s) that the information relates to where appropriate;
- where we rely on legitimate interests as our lawful reason for processing, ensure a legitimate interests assessment (LIA) is carried out to ensure we can justify our decision;
- where sensitive personal information is processed, also identify a lawful special condition for processing that information (see Sensitive personal information below), and document it; and
- where criminal records information is processed, also identify a lawful condition for processing that information, and document it (see criminal records information below).

Where you process personal information on our behalf, you must ensure that you comply with the above requirements in order to help us meet our obligations. If future processing is likely to result in a high risk to an individual's data protection rights (e.g. where we plan to use a new form of technology or process sensitive personal information on a large scale), we will, before starting the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, or other potentially high-risk processing is carried out, the manager responsible should contact the DGM at legalservices@thalia.co.uk in good time, so that a DPIA can be carried out, if appropriate.

We keep a record of our processing activities in accordance with our obligations.

Sensitive personal information

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'. We recognise that processing sensitive data requires additional measures.

We may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- we have a lawful reason for doing so, as set out above, e.g. it is necessary for the performance of the employment contract, to comply with our legal obligations or for the purposes of our legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, for example:
    - the data subject has given explicit consent (this will only apply in limited circumstances);
    - processing is necessary for the purposes of exercising the employment rights or obligations of Thalia Waste Management or the data subject;
    - processing is necessary to protect the data subject's vital interests, and the data subject is physically or legally incapable of giving consent;
    - processing relates to personal information which is manifestly made public by the data subject;
    - processing is necessary for the establishment, exercise or defence of legal claims; or
    - processing is necessary for reasons of substantial public interest.

In order to help us meet our obligations, whenever you process sensitive personal information on our behalf, you must ensure that you comply with the requirements set out above and elsewhere in this Policy, including that there is a valid lawful reason for the processing and one of the special conditions for processing sensitive personal information applies. If you are in any doubt about whether the information can be lawfully processed, please contact the DGM at legalservices@thalia.co.uk.

The Privacy Notice sets out the types of sensitive personal information that we process about our workforce, what it is used for and the lawful basis for the processing.

We will comply with this Policy and our related policies and procedures to ensure that we comply with the Data Protection Principles when we process sensitive personal information.

Generally, we will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information. However, where in the limited circumstances we do carry out automated decision the individual concerned will be informed of the logic involved in the decision making, the significance and envisaged consequences and give the individual the right to request human intervention, express their point of view or challenge the decision-making.

Criminal records information

We will only collect, store and use information about criminal convictions and offences if it is appropriate, given the nature of your role, and provided we are legally able to do so. Where appropriate, we will process information about criminal convictions and offences as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. The Privacy Notice gives further details about how we obtain and use criminal records information about our workforce.

Where we process criminal records information, we will follow this Policy and our related policies and procedures to ensure that we comply with the Data Protection Principles.

Privacy Notices for Existing and New Personal Data

We will issue privacy notices from time to time. These inform you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes. We aim to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Whenever we first obtain personal information directly from an individual, we must also ensure that an appropriate privacy notice is provided to them. When personal information is obtained indirectly (for example, from a third party or publicly available source), we are required to provide the individual with certain information as soon as possible after we receive the data. We must also check that the personal information was collected lawfully and on a basis which envisages our proposed use of that information.

You should contact the Information Governance Team at legalservices@thalia.co.uk for further guidance whenever you are obtaining personal data for the first time, whether directly or indirectly, in the course of your role, to ensure we comply with our obligations to provide information about that personal data collection.

Where we enter into a new contract with a new or existing customer or with a new or existing subcontractor, you should ensure that the contract(s) contain appropriate provisions reflecting our obligations under GDPR. You should ensure that our Legal team have approved the provisions dealing with personal data and that any necessary approvals have been obtained.

Individual rights

You, as well as others, have the following rights in relation to your personal information (amongst others and subject to certain exemptions):

- to be informed about how and why your personal information is processed - see the Privacy Notice;
- to make a data subject access request to obtain a copy of the personal information we hold about you and other information;

- to have personal data corrected if it is inaccurate or incomplete;
- to have personal data erased in certain circumstances e.g. if it is no longer necessary for the purpose for which it was collected or there are no overriding legitimate grounds for the processing;
- to restrict the processing of personal information in certain circumstances e.g. where the accuracy of the information is contested, or the processing is unlawful (but erasure of the information is not appropriate), or where we no longer need the personal information, but it is required to establish, exercise or defend a legal claim;
- to ask to obtain a portable copy of those parts of your personal data where we rely on consent or performance of the contract as the justification for processing, or to have a copy of that personal data transferred to a third-party controller; and
- to object to processing which we have justified on the basis of a legitimate interest - in which case the relevant processing will only continue if it has become necessary for us to continue processing that personal information; and
- to object to any decisions based solely on automated decision making.

If you wish to exercise any of the rights listed above or have any questions, please refer to the Privacy Notice in the first instance.

If you receive a written request from a third party of the nature set out above, you should forward it to the Information Governance Team at legalservices@thalia.co.uk immediately.

Information security

We will use appropriate technical and organisational measures to keep all data secure and shall protect such data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where appropriate, personal information is either anonymised, pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident impacting on personal information held by us, availability and access to personal information can be restored in a timely manner;
- ensuring a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; and
- implementing new systems and process incorporate ‘Privacy by Design’.

Our Information Security Management Policy sets out further details in relation to information security.

Where we use external organisations to process personal information on our behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered or extended, the guidance must be followed and any necessary approvals must be obtained. We must ensure we are meeting all of our data protection obligations in relation to that information.

Data Breaches and Process

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which information is stored;
- unauthorised access to or use of information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental disclosure, deletion or alteration of data;
- successful/effective attacks on IT systems, such as hacking, viruses or phishing scams; and
- theft by deception, where information is obtained by deceiving a member of the organisation which holds it.

Where the data breach results in the disclosure of personal data, we will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

If you know or suspect that a data breach has occurred, you must immediately inform your line manager who should then immediately notify the IT Service Desk by telephone on 01276 455 455. If you cannot notify your line manager immediately, you should immediately notify the IT Service Desk on 01276 455 455.

When reporting the suspected breach, provide as much detail as possible, including dates and times of the suspected breach, along with specific detail of information breached and any associated volumes.

Do not attempt to investigate the matter yourself. You should preserve all evidence relating to the potential data breach.

Training

We will ensure that our workforce is adequately trained on their data protection responsibilities. Individuals whose roles require regular access to personal information, 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.

Storage, Retention and Disposable Information

Storage

Our preferred storage medium is electronic storage rather than physical storage. All physical data, including handwritten documents should be scanned and archived electronically.

Where it is essential for a physical copy to be kept, then such data should have an electronic copy made for electronic storage and the physical copy be stored in a fireproof environment using one of our approved suppliers.

Each account or function is responsible for the control of its own data.

Retention

The length of time for which data should be retained will depend upon the circumstances, including the reasons why the data was obtained and any relevant legal, regulatory or business considerations. The Document Retention Schedule, which is available to Data Users on Thalia Waste Management's intranet, sets out the period of time data must be retained for. Data must not be retained beyond the period indicated in the Document Retention Schedule, unless a valid business reason (for example, a stop order has been issued by the General Counsel) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Information Governance Manager who will offer the necessary guidance. Records will be securely deleted or destroyed after the end of the relevant retention period.

When the retention period has lapsed for contracts, you should seek clearance from our Legal team before arranging for the disposal of the document.

Data with a retention time exceeding two years, to which current access is not required, should be considered for archival storage. Please refer to the Document Retention Schedule.

You must help us comply with our obligations in relation to the storage and retention of personal data by not keeping personal information in a form which enables the identification of the person it relates to for longer than needed for the legitimate business purpose(s) for which we collected it.

Data must be retained beyond the Retention Period in the following circumstances:

- **if legal proceedings have been threatened or commenced, or where there is a reasonable anticipation that such proceedings may be brought, in respect of which the document may be relevant;**
- **the document is relevant to a company in liquidation or receivership;**
- **the General Counsel has issued a "stop" order on the destruction of the document**

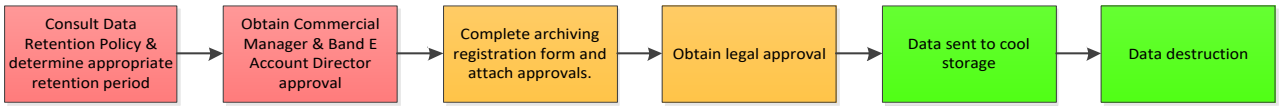
Disposable information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Document Retention Schedule. Examples may include:

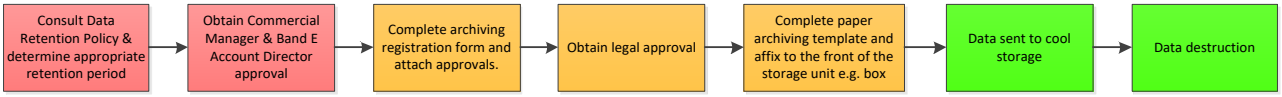
1. Duplicates of originals that have not been annotated.
2. Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
3. Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Thalia Waste Management and retained primarily for reference purposes.
4. Spam and junk mail.

If a document is not listed in the Document Retention Schedule, if you are uncertain on any aspect of document storage, retention or disposal or if you have any general queries in relation to personal data, please contact the Data Governance Manager at legalservices@thalia.co.uk.

Process for handling electronic data



Process for handling physical data



Confidential information belonging to others

From time to time, we enter into Non-Disclosure Agreements with third parties pursuant to which we will possess information which we are obliged to keep confidential. Such information must not, so long as such information remains confidential, be disclosed by us. At the end of the agreed period, or on the earlier termination of the Non-Disclosure Agreement, we usually have to either return such confidential information or undertake to have disposed of such data. The Non-Disclosure Agreement must be followed and it must be possible to evidence our compliance with such agreement.

Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

Paco Hevia

Chief Executive

November 2022

Revision Status

Revision	Date	Amendment	Content Owner	Mandated By
1.0	Nov 22	Issued for use	Janet McDonald	Paco Hevia