DORMOLE LTD

Policy Document

Title	Version	Author	Date	Review Date
Data Protection Policy	1.3	Wendy Milne-Bennett	04-March-2019	As Required

1. Introduction

Dormole Limited and its subsidiaries (the "**Dormole Group**" and each a "**Dormole Group Company**") are required to obtain and keep a certain amount of Personal Data in order to perform their day to day businesses and to meet their legal obligations to both their employees and customers. This Policy sets out how each Dormole Group Company handles the Personal Data of its employees, workers, customers, suppliers and other third parties.

This Policy has been approved by the Dormole Limited Board. This Policy applies to all Dormole Group Company personnel (including employees, contractors consultants, workers, directors and others). All personnel must comply with this Policy when processing Personal Data on behalf of a Dormole Group Company and personnel's compliance with this Policy is mandatory. Any breach of this Policy will be taken seriously and may result in disciplinary action.

Dormole Group reserves the right to change this Policy at any time without notice so please check back regularly to obtain and familiarise yourself with the latest version of this Policy. This Policy was last revised on **4th March 2019.**

2. Definitions of Data Protection terms

Data Subjects, for the purpose of this Policy, include all living individuals about whom Dormole Group Companies hold Personal Data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their Personal Data.

Personal Data is defined as any information relating to a person who can be identified directly or indirectly from that data. This definition includes Personal Data held in both electronic and paper format. Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour and it can include CCTV images used in the course of a Dormole Group Company's business.

Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the applicable data protection legislation. Each Dormole Group Company is the Data Controller of all Personal Data used in its business for its own commercial purposes, including Personal Data relating to its employees (except in certain instances where Dormole Limited acts as a Data Processor on behalf of other Dormole Group Companies).

Data Processors in the case of each Dormole Group Company include any person or organisation that processes Personal Data on that company's behalf and on that company's instructions. Employees of Data Controllers are excluded from this definition, but it could include suppliers which handle Personal Data on that company's behalf, such as organisations appointed to administer the Dormole Group's pension schemes. In some instances, a Dormole Group Company may be a Data Processor on behalf of others.

Personal Data Breach is any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that are put in place to protect it. It also includes the loss of, or unauthorised access, disclosure or acquisition of Personal Data.

Processing (or "**Processed**" or similar expression) is any activity that involves use of the Personal Data. It includes obtaining, recording or holding the Personal Data, or carrying out any operation or set of operations on the Personal Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

Special Categories of Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life or sexual orientation, genetics or biometrics. Special Categories of Personal Data can only be processed under strict conditions, including a condition requiring the explicit consent of the Data Subject.

In this Policy, unless the context otherwise requires, references to 'Personal Data' includes 'Special Categories of Personal Data'.

3. Data Protection Manager

The Dormole Group fully accepts its responsibilities and has appointed Wendy Milne-Bennett as its data protection manager.

The data protection manager is responsible for carrying out regular Data Protection Impact Assessments and dealing with and for reporting any Personal Data Breach to the Information Commissioner's Office.

If anyone has any questions in relation to data protection or has any concerns that the Dormole Group or any Dormole Group Company is not fulfilling its obligations under the data protection legislation, they should contact the data protection manager who will be responsible for investigating the matter.

4. Data Protection Principles

The data protection legislation sets out basic principles which those processing Personal Data should abide by to ensure that any Personal Data they keep is held securely and processed in the correct manner.

Each Dormole Group Company is committed to ensuring that it abides by these principles.

The main principles are as follows;

a. The Personal Data must be processed fairly, lawfully and transparently.
b. The Personal Data must be collected and processed for specified, explicit and legitimate purposes.
c. The Personal Data held must be adequate and relevant and limited to what is necessary for the purposes for which it is processed (this is also commonly referred to as "data minimisation").
d. The Personal Data must be accurate and, where necessary, kept up to date.
e. The Personal Data should not be held for longer than is necessary.
f. The Personal Data should be securely stored and access limited to those who need it.

In addition to the above 6 principles which are set out in the data protection legislation, we are also committed to not transferring Personal Data outside of the EEA unless appropriate safeguards are in place (see section 12 below) and to allow Data Subjects to exercise their rights under the data protection legislation in relation to the Personal Data which the Dormole Group hold about them (see section 13 below).

We have set out below in more detail how we deal with Personal Data in order to comply with the above principles.

5. Data Security

The Dormole Group fully accepts its responsibility to ensure that all Personal Data is held securely. To that end, appropriate security, technological and organisational measures will be taken against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

Impact assessments and commissions are carried out as well as regular external audits of Dormole Group Companies' systems and networks to ensure that we implement and maintain safeguards appropriate to the size, scope and business of

the relevant Dormole Group Company, resources available, the amount of Personal Data which is held and any identified risks. The findings of these impact assessments, commissions and audits are recorded and, in the event that potential issues are identified, the appropriate remedial action is taken.

Each Dormole Group Company will train all personnel who have been authorised to access any form of Personal Data on the relevant company's protocols, procedures and technologies for ensuring that the Personal Data is properly safeguarded, and personnel must comply with and follow them. Personnel must exercise particular care in respect of processing of any Special Categories of Personal Data.

These protocols include;

a. Having a clear understanding of the definitions of Personal Data.
b. Ensuring that only those personnel who need to know and are authorised to use Personal Data have access to it.
c. Complying with all security measures set out in the Dormole IT Policy
d. Only transferring Personal Data to third parties which agree to adequate measures being in place (see section 12 below).
e. If personnel know or suspect that a Personal Data Breach has occurred, complying with section 6 below.
f. Avoiding the copying of Personal Data to external systems, including 'flash drives' unless absolutely necessary.
g. Avoiding the use of email as a method of transferring Personal Data if at all possible.
h. Ensuring that all Personal Data, both in electronic and paper form, is stored securely. In the case of paper records, this means keeping Personal Data behind two locked doors. In the case of electronic records, this means storing data in secure locations approved by the HR Department and ensuring that all files are protected by strong passwords.
i. Keeping the Personal Data accurate and in good order and identifying Personal Data that is no longer required.
j. Ensuring that all Personal Data which is no longer required is destroyed in an acceptable manner and in line with the procedures set out in Schedule 1.

In addition to the above, each Dormole Group Company must implement privacy by design measures when processing Personal Data by implementing appropriate organisational and technical measures. Each Dormole Group Company should assess what privacy by design measures can be implemented on all processes, systems and programs taking into account the state of the art, the cost of implementation, the nature of the processing and the risks to Data Subjects which is posed by the processing.

Each Dormole Group Company must carry out a Data Protection Impact Assessment when implementing any major system or business change programs which involve Personal Data and which:

a. use new or changing technologies;

b. involve profiling or automated decision making; or
c. involve large scale processing of Special Categories of Personal Data.

Each Dormole Group Company should discuss any proposed Data Protection Impact Assessment and its results with the data protection manager (see section 3 above) to ensure compliance with the data protection legislation.

6. Data Breaches

Data protection legislation requires Data Controllers to inform the applicable regulator and in certain circumstances the Data Subject of any Personal Data Breach.

If personnel know or suspect that a Personal Data Breach has occurred, they should not attempt to investigate the matter themselves. Personnel should immediately contact the data protection manager (see section 3 above) who will activate the relevant Dormole Group Company's procedures. Personnel and each Dormole Group Company should preserve all evidence relating to any potential Personal Data Breach.

7. Lawfulness and Fairness

Any Personal Data which the Dormole Group process must be processed lawfully, fairly and transparently.

Data protection legislation requires that Personal Data may only be processed for a lawful purpose. Those lawful purposes include:

a. the processing is necessary in relation to a contract which has been entered into with the Data Subject;
b. it is necessary to meet Dormole Group's legal obligations;
c. it is to pursue our legitimate interests (so long as those interests do not override the interests or rights of the Data Subject); or
d. the Data Subject has given their consent to processing (see below for more details on consent).

Dormole Group must set out in its privacy notices the lawful purpose on which it is processing Personal Data. These privacy notices will be available to Data Subjects so that they can understand how their Personal Data is processed by the relevant Dormole Group Company (see section 8 below for more details).

Personal Data must not be processed in a way that is incompatible with the lawful purpose which was originally told to the Data Subject, unless they have been informed of the new purpose, and where relevant, consented to that new purpose.

Consent

In the very limited instances where we would rely on consent as the lawful purpose for processing a Data Subject's Personal Data then we must gain that person's consent in a clear way. Data protection legislation requires this consent to be given by positive action. This means that silence, pre-ticked boxes or inactivity will not constitute consent. If Data Subject's give their consent as part of another document, then the consent should be separate from those other matters.

Data Subjects can withdraw their consent to us processing Personal Data for which they have given us their consent to hold at any time and no processing of this Personal Data should occur once they have withdrawn their consent. If their Personal Data is to be processed for a different and incompatible purpose to the one originally given to them when processing first began, then the Data Subject should be updated and consent should be refreshed.

If a Dormole Group Company relies on consent as the lawful purpose for processing Special Categories of Personal Data or for transferring Personal Data outside of the EEA (see section 12 below) then that consent must be explicit. Explicit consent requires a clear and specific statement from the Data Subject. However, if Dormole Group Companies want to do these things, it will usually rely on another lawful purpose (other than consent) to do them.

If a Dormole Group Company does rely on consent as the lawful purpose then it must keep a record of the consent which includes the time, date and means by which consent was obtained and what information the Data Subject was given (for example, a privacy notice).

8. Transparency and Privacy Notices

A key part of the data protection legislation is about being transparent with Data Subject's about the collection and processing of their Personal Data. The Dormole Group will inform Data Subjects about this via a privacy notice. These privacy notices include those matters which Data Controllers must tell a Data Subject about under the data protection legislation.

If a Dormole Group Company collects the Personal Data directly from a Data Subject then the relevant privacy notice should be available to the Data Subject when the Personal Data is first collected.

If a Dormole Group Company collects the Personal Data indirectly (for example from a third party) then it must provide the privacy notice to the Data Subject as soon as possible after receiving the Personal Data. If a Dormole Group Company receives Personal Data indirectly from a third party it should ensure that that third party has collected the Personal Data in accordance with the data protection legislation and that such collection by the third party covers the processing which the Dormole Group Company is to carry out.

Copies of the relevant privacy notices can be accessed via the Dormole Group Intranet and are available from the Dormole Group's HR Department (0121 502 9381 or hr@toolbank.com). This includes a privacy notice about how the Dormole Group process personal data relating to employees, workers and contractors.

9. Data Minimisation

Each Dormole Group Company should only collect Personal Data to the extent that it is necessary for the reasons for which it is collected. Collection of Personal Data should not be excessive.

Personnel must only process Personal Data where it is required for their job duties and they must not process it for any reasons which are unrelated to their job duties.

10. Accuracy

Each Dormole Group Company must ensure that any Personal Data which it holds is accurate, complete and up to date. Each Dormole Group Company should check the accuracy of Personal Data when it is collected and at regular intervals thereafter.

Any incorrect or out of date Personal Data must be corrected, deleted or destroyed promptly and without undue delay.

11. Data Retention

Personal Data which allows for Data Subjects to be identified should not be kept longer than is necessary for the reasons it was collected or for longer than is needed for the legitimate business purposes of the relevant Dormole Group Company (including any legal and accounting reasons).

If Personal Data is no longer required, then it must be anonymised or deleted in accordance with the Dormole Group's retention criteria which are set out in Schedule 1 to this Policy. Each Dormole Group Company should also require any third parties, including third party processors, to delete any such Personal Data, where applicable.

All privacy notices will include information about the period for which Data Subjects' Personal Data will be stored.

12. Third Party Disclosures

Dormole Group Companies keep a register of all the third parties (companies and individuals) to whom they send Personal Data. The register details the type of information sent, the reason as to why it is sent and as to how it is used and the way in which it is transferred. This information is available on the Dormole Group Intranet or from the Dormole Group HR Department.

Personal Data may only be shared with third parties if certain safeguards and contractual arrangements have been put in place. All third parties referred to above are required to sign a Data Sharing Agreement (or have provided us with an appropriate contractual arrangement) which will ensure that they are handling any Personal Data in the correct manner and in compliance with the data protection legislation.

Personal Data may only be shared with third parties (such as service providers) if:

a. that third party needs to know the Personal Data for the purposes of providing a contracted service;
b. sharing the Personal Data complies with any privacy notice provided to the Data Subject (see section 8 above);
c. that third party has agreed to comply with required data security standards policies and procedures and has put adequate measures in place;
d. there is in place a written contract that contains data protection legislation compliant clauses; and
e. (only if Personal Data is to be transferred outside of the EEA), applicable safeguards are in place (see the following paragraphs for more details).

Dormole Group Companies must not provide Personal Data to any third party which would involve the transfer, access, viewing or transmitting of Personal Data outside of the EEA unless one of the following conditions applies:

a. the EU Commission has provided a decision that the country in question ensures an adequate level of protection for Data Subjects;
b. appropriate safeguards are in place which include standard contractual clauses approved by the EU Commission, binding corporate rules, an approved code of conduct or certification mechanism;
c. the Data Subject has provided their explicit consent to the transfer (see section 7);
d. the transfer is necessary for one of the other reasons set out in the data protection legislation which include the performance of a contract between the relevant Dormole Group Company and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims, to protect the vital interests of the Data Subject and in some other limited cases, for the relevant Dormole Group Company's legitimate interest.

Dormole Group Companies may share Personal Data they hold with any other Dormole Group Company to enable the receiving Company to perform legal or contractual obligations on its behalf, as part of regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data and in each case so long as the employee or representative of that other Dormole Group Company has a job-related need to know the information. In every case where this applies, the Dormole Group Companies will enter into a Data Sharing Agreement.

In addition to the above, Personal Data may be disclosed to third parties:

a. in the event of a sale or purchase of any business or assets owned within the Dormole Group, in which Personal Data may be disclosed to the prospective seller or buyer of such business or assets; or
b. if a Dormole Group company or substantially all of its assets are acquired by a third party, in which case Personal Data it holds will be one of the transferred assets.

Dormole Group Companies may disclose Personal Data if under a duty to disclose or share Personal Data in order to comply with any legal obligation.

13. Data Subject's rights in respect of Personal Data

Data Subjects have rights in respect of the Personal Data held and processed by any relevant Dormole Group Company. These rights include:

a. requesting access to the Personal Data held about them (see below for more details);
b. withdrawing their consent to processing (where the relevant Dormole Group Company has relied on consent as the lawful basis for processing their Personal Data);
c. receiving certain information about processing activities;
d. preventing use of Personal Data for direct marketing purposes;
e. requesting erasure of Personal Data if it is no longer necessary, requesting rectification of inaccurate Personal Data or completion of incomplete Personal Data;
f. requesting for processing to be restricted in specific circumstances;
g. challenging processing where the lawful purpose has been stated to be the legitimate interests of the relevant Dormole Group Company;
h. requesting a copy of any agreement under which Personal Data is transferred outside of the EEA;
i. preventing processing that is likely to cause damage or distress to the Data Subject or somebody else;
j. to be notified of a Personal Data Breach where it is likely to result in a high risk to the rights and freedoms to Data Subjects; or
k. to make a complaint to the relevant data protection regulator (in the UK this is the Information Commissioner's Office).

Any request to exercise a Data Subject's rights should immediately be passed to the data protection manager (see section 3 above).

In relation to a request for access to Personal Data, the relevant Dormole Group Company processing the Personal Data will need to meet its obligations by making the requested Personal Data available to the Data Subject in line with the data protection legislation and without undue delay and, at the latest, within one month of receipt of the request.

14. Record Keeping

Data protection legislation requires each Dormole Group Company to keep details of its processing activities.

Records should include as a minimum: the name and contact details of the Data Controller and the relevant data protection manager; clear descriptions of the types of Personal Data; categories of Data Subjects; processing activities; the lawful purpose for processing; third party transfers; storage locations; retention periods and descriptions of the security measures in place.

An up to date version of these records are available on the Dormole Group Intranet or from the Dormole Group's HR Department.

15. CCTV

The following paragraphs set out the Dormole Group policy in relation to CCTV, although other paragraphs of this policy will also be relevant to the personal data captured by any CCTV (such as section 5 relating to data security).

Dormole Group believes that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all staff and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy.

Dormole Group currently use CCTV cameras to view and record events and individuals in or around our premises.

Dormole Group recognises that images of individuals recorded by CCTV cameras in the workplace are Personal Data and therefore subject to data protection legislation.

We have set out in in our privacy notices the reasons for which we use CCTV and the lawful reason on which we are relying to do so. The reasons we use CCTV include ensuring that the buildings and stock are safe and secure and that those on the premises are behaving in a safe and responsible manner.

CCTV monitors parts of the interior and exterior of the building and details of where they are sited are available at each location. Generally, they are in operation 24 hours a day and this data is continuously recorded. Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property. Surveillance systems will not be used to record sound.

Images may be accessed and monitored by authorised personnel every day of the year.

Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a Data Protection Impact Assessment.

Covert Monitoring

We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Managing Director or Chief Executive Officer of the relevant Dormole Group Company. The decision to carry out covert monitoring will be fully documented and will include a Data Protection Impact Assessment and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

16. EPOD Proof of Delivery System and Vehicle Trackers

The EPOD proof of delivery system is a handheld device which is used by some of our employees, agency workers, and workers whose jobs involve delivery of products.

The EPOD proof of delivery system records the driver's route and can track their location as well as information such as the distance the vehicle has covered. It also provides evidence as to the proof of delivery of products to their destination as it records signatures by those who receive the deliveries as well as a time stamp as to when the delivery occurred.

In exceptional circumstances, vehicle trackers may be fitted to vehicles. Vehicle trackers record the driver's route and can track their location as well as information

such as the distance the vehicle has covered. This is only done with the express authorisation of the Managing Director or Chief Executive Officer of the relevant Dormole Group Company. The decision to carry out vehicle tracking will be fully documented and will include a Data Protection Impact Assessment. We will consult with the relevant employee(s) and/or worker(s) where a vehicle tracker is proposed to be fitted to a vehicle which they use, including details as to the purposes it will be used and the lawful basis for us processing such Personal Data.

If you have been authorised to use a company vehicle outside of working hours and you have an EPOD proof of delivery system device with you (i.e. it has not been returned to the branch following your last delivery) then you must ensure that the EPOD proof of delivery system device is switched off for any journeys which you make outside of your working time. You must keep the EPOD proof of delivery system device switched on during working hours and it may be a disciplinary offence if you turn it off during working hours.

If you have been authorised to use a company vehicle outside of working hours and the vehicle which you are using is fitted with a vehicle tracker, then those vehicle trackers will be fitted with privacy buttons which allow you to switch off the device for journeys outside of your working time. You are responsible for ensuring that this is switched off. If it is switched off during working hours, it may be a disciplinary offence.

If for any reason you have forgotten to switch off the EPOD proof of delivery system device or vehicle tracker for any journeys outside of working hours, please contact your line manager and provide details so that such data may be deleted from the system.

The data recorded from the EPOD proof of delivery system device is used for the following reasons:

- to track the mileage of vehicles in order to ensure that the vehicles are within the remits of insurance policies taken out in respect of them;

- to record the delivery details of products, including the time they were delivered and the person who received the delivery. This information assists the relevant Dormole Group Company in proving that delivery occurred and by whom should a query be raised by a customer of the relevant Dormole Group Company;

- to record the number of driving hours completed by the relevant employee or worker to ensure that the relevant Dormole Group Company is in line with legal obligations;

- to allow us to estimate times of delivery to customers based on the current location of the relevant employee/worker, including to advise customers if deliveries are likely to be late;

- to ensure that all customer deliveries are made in the most efficient manner.
- in the case of unusual patterns of activity or non-activity, to investigate the reasons for this.

If we use data from the EPOD proof of delivery system device or vehicle tracker in respect of unusual patterns or activity or non-activity, then we may use this as evidence in any subsequent disciplinary process. We will consult with relevant HR or legal advisers, if such evidence is to be used, in order to establish whether it is essential to the investigations.

Dormole Group Companies will identify in the relevant privacy notices the lawful basis for us processing Personal Data from the EPOD proof of delivery system device or vehicle tracker which will usually be because the relevant Dormole Group Company has a legal obligation to obtain such data or because it is in the legitimate interests of the relevant Dormole Group Company.

Schedule 1 - Retention Periods and Deletion

Part 1 - Retention Periods

Type	Type of Personal Data	Retention Period	Notes
Unsuccessful candidates for roles	Job Application, CV and Interview Notes	6 months after notifying candidates of the outcome of the recruitment process	
Employee	Job Application, CV and Interview Notes	7 Years after leaving	
Employee	Offer Letter and Starter Forms	7 Years after leaving	
Employee	References	7 Years after leaving	
Employee	Contract of Employment	7 Years after leaving	
Employee	Employee Details (including DOB, NI number and Nationality)	7 years after leaving	
Employee	Employee Contact Details	1 Year after leaving	
Employee	Next of Kin	1 Year after leaving	
Employee	Bank Details	2 Months after leaving	
Employee	Company Equipment issued	6 Months after leaving	
Employee	Job Description	7 years after leaving	
Employee	Holiday Entitlement	7 Years after leaving	
Employee	Job and Salary Details	7 Years after leaving	
Employee	Bonus and Commission Details	7 Years after leaving	These must be kept for 3 Years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for 7 Years after leaving.
Employee	Benefits (Life Assurance, PHI, Childcare etc.)	7 Years after leaving	These must be kept for 3 Years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for 7 Years after leaving.
Employee	Gender Pay Details	1 Year after leaving	
Employee	Work Performance Statistics	7 years	

Type	Type of Personal Data	Retention Period	Notes
Employee	Expression of Wish	7 Years after leaving	
Employee	Time and Attendance records	7 Years after leaving	These must be kept for 3 Years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for 7 Years after leaving.
Employee	Pension Details	7 Years after leaving for Group Pension Plan	For members of TRBS pension, details will be retained for the lifetime of the scheme under the Trust Rules which is until the last member of the scheme dies and they will be retained until the scheme is dissolved following the death of the last member.
Employee	Absence from Work	7 Years after leaving	These must be kept for 3 Years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for 7 Years after leaving.
Employee	Disciplinary records	7 Years after leaving	
Employee	Grievance Notes	7 Years after leaving	
Employee	Manager's Notes	7 Years after leaving	
Employee	Medical Condition	7 Years after leaving	
Employee	Training detail and qualifications	6 Months after leaving	
Employee	Annual Appraisals	7 Years after leaving	
Employee	Driving Details (including licence details)	6 Months after leaving	
Employee	Company Vehicle	6 Months after leaving	
Employee	Company Vehicle Accident Records	5 Years after accident	
Employee	Maternity/Paternity Leave	4 Years after the end of the tax year in which the maternity pay period ends.	

Type	Type of Personal Data	Retention Period	Notes
Employee	Company Loan Details	6 Months after leaving	
Employee	Leaving Records	7 Years after leaving	
Employee	Payroll Details	7 Years after leaving	These must be kept for at least 3 Years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for 7 Years after leaving.
Employee	CCTV Data	7 Years after investigation	CCTV is only stored and retained for use in any investigations, if required. In normal circumstances, CCTV footage will be recorded over and not retained.
Employee	EPOD proof of delivery system device or vehicle tracker data	7 Years	
Customer	Drop Ship - Consumer Address Details	3 Months from the end of the month in which the goods were dispatched	

(Nb. A Data Register detailing all the Personal Data fields held by the Dormole Group of Companies is available on the Dormole Group Intranet or from the Dormole HR Department).

Part 2 - Deletion Methods

The Dormole Group of Companies will delete Personal Data once it is no longer required and in accordance with Schedule 1 of this policy. Electronic Data is deleted from the systems based on an automatic deletion schedule in line with the time periods laid out above. Paper records are shredded using a cross cutting shredder with a P-4 security level.