Wasteland Ski

Data Retention Policy

CONTENTS

CLAUSE

1. ABOUT THIS POLICY 1
2. SCOPE OF POLICY 1
3. GUIDING PRINCIPLES 1
4. ROLES AND RESPONSIBILITIES 1
5. TYPES OF DATA AND DATA CLASSIFICATIONS 2
6. RETENTION PERIODS 2
7. STORAGE AND DISPOSAL OF DATA 3
8. SPECIAL CIRCUMSTANCES 3
9. WHERE TO GO FOR ADVICE AND QUESTIONS 3
10. BREACH REPORTING AND AUDIT 4
11. OTHER RELEVANT POLICIES 4

ANNEX

ANNEX A DEFINITIONS 5
ANNEX B RECORD RETENTION SCHEDULE 6

1. ABOUT THIS POLICY

1.1 This Data Retention Policy explains Wasteland's requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. SCOPE OF POLICY

2.1 This policy covers all personal data that we hold or have control over. This includes electronic data such as emails and electronic documents. It also includes physical data such as hard copy documents, contracts, notebooks and letters. In this policy we refer to this information and these records collectively as "data".

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

3. GUIDING PRINCIPLES

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

4. ROLES AND RESPONSIBILITIES

4.1 **Responsibility of all employees**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Record Retention Schedule, any communications suspending data

disposal and any specific instructions from the DPO (**Gareth Hunter** is our DPO). A member of staff's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 The DPO is responsible for:

- Administering the data management programme;
- Developing data disposal policies and procedures; and
- Providing guidance in relation to this policy.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **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 Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- 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.
- Spam and junk mail.

Please see paragraph 6.2 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 6.3 below for more information on this.

6. RETENTION PERIODS

6.1 **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the DPO.

6.2 **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for

business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data.

6.4 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the DPO.

7. STORAGE AND DISPOSAL OF DATA

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner.

7.2 **Destruction**. The destruction of personal hard copy data must be conducted by shredding.

7.3 The destruction of data must stop immediately upon notification from the DPO.

8. SPECIAL CIRCUMSTANCES

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all staff to comply fully with our Record Retention Schedule and procedures as provided in this policy. All staff should note the following general exception to any stated destruction schedule: If you believe that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the DPO determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept. This is especially relevant if Wasteland has signed a services contract with a customer that is subject to a law other than the laws of England & Wales because foreign laws may enable customers to bring claims against Wasteland outside the limitation periods referred to in the Record Retention Schedule.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the DPO.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

Questions about the policy. Any questions about this policy should be referred to the DPO, who is in charge of administering, enforcing, and updating this policy.

10. BREACH REPORTING AND AUDIT

10.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on staff. If you feel that you or someone else may have breached this policy, you should report the incident immediately to the DPO. If staff do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

10.2 No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3 **Audits**. We will regularly monitor compliance with this policy, including by carrying out audits. We will carry out an annual review of all of the personal data that we collect in connection with the services that we supply to our customers to determine whether the retention policy that we have adopted for that personal data is still appropriate.

11. OTHER RELEVANT POLICIES

This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time.

ANNEX A DEFINITIONS

Data: all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks and letters. It also includes electronic data such as emails, electronic documents, audio and video recordings. It applies to personal data only. In this policy we refer to this information and these records collectively as "data".

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO with responsibility for data protection compliance. Our current DPO is **Gareth Hunter**.

Data Retention Policy: this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

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 Record Retention Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Personal data: any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Record Retention Schedule: the schedule attached to this policy which sets out retention periods for our formal or official records.

Sensitive personal data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

Storage limitation principle: data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the GDPR as the principle of storage limitation.

ANNEX B RECORD RETENTION SCHEDULE

Wasteland establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance and accomplish other objectives, such as controlling costs.

Staff should comply with the retention periods listed in the record retention schedule below, in accordance with Wasteland's Data Retention Policy.

If you hold data not listed below, please refer to Wasteland's Data Retention Policy and, specifically, the section dealing with disposable records. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact Gareth Hunter.

TYPE OF DATA	RETENTION PERIOD	REASON / COMMENTS
Emails / correspondence with our customers or suppliers.	6 years 6 months following completion of the business to which they relate – unless emails/correspondence with our suppliers or subcontractors relates to investigations that require longer periods of retention (see below).	6 years is the limitation period within which to bring breach of contract / negligence claims. We have added a cushion of 6 months in case of litigation at the end of the period.
Emails / correspondence with our potential customers.	2 years from last contact.	We may receive business from potential customers within 2 years of last contact and previous correspondence with them may be relevant to the terms of business that we may have previously offered them.
Emails / correspondence with our potential suppliers.	2 years from last contact.	We may place business with potential suppliers or subcontractors within 2 years of last contact and previous correspondence with them may be relevant to the terms of business under which we work with them.
Emails/ correspondence / documents exchanged with our professional advisers such as our	15 years 6 months from the end of the matter which the data	15 years is the long stop date within which to bring professional negligence cases. We have

lawyers and accountants.	relates to.	added a cushion of 6 months in case of litigation at the end of the period.
Documents that have been signed using Wasteland's seal or which have been signed as a deed or which relate to a mortgage or charge or a land dispute.	12 years 6 months from the date of the document.	12 years is the long stop date within which to bring claims. We have added a cushion of 6 months in case of litigation at the end of the period.
Documents relating to the establishment of Wasteland. Tax registration documents, records and filings. Trademark registrations or other registrations of intellectual property. Domain name registrations. Our policies and procedures. Bank account details and bank statements. Records of filings at Companies House or at registrars in other jurisdictions and minutes of meetings of the directors or shareholders of Wasteland. Correspondence and documents relating to our pension scheme.	Do not destroy.	We may need these documents as evidence of compliance with our legal obligations or to protect our intellectual property.
Contracts that do not fall under any of the categories above.	6 years 6 months from the termination date of the contract.	6 years is the limitation period within which to bring breach of contract / negligence claims. We have added a cushion of 6 months in case of litigation at the end of the period.
Insurance documents / Health and Safety records.	6 years 6 months from the termination date of the insurance cover / health and safety incident.	6 years is the limitation period within which to bring negligence claims. We have added a cushion of 6 months in case of litigation at the end of the period.
Correspondence with and documentation relating to any investigation made by the police, or any regulator or government	Do not destroy.	We may need to retain this information indefinitely – contact the DPO.

department, for example The Information Commissioner's Office or HMRC.		
Documentation relating to breach of data protection law, data security breaches and requests, notices or claims received regarding compliance with data protection laws.	6 years 6 months from the termination date of the insurance cover / health and safety incident.	6 years is the limitation period within which to bring claims. We have added a cushion of 6 months in case of litigation at the end of the period.
Correspondence or documentation relating to any litigation involving Wasteland.	Do not destroy.	We may need to retain this information indefinitely – contact the DPO.
A member of staff's government identification numbers / bank account details / payroll information / wage and benefit information.	3 years 3 months from the end of the tax record they relate to.	Legal requirement to retain information for this period. We have added a cushion of 3 months in case of any issues raised by HMRC.
A member of staff's passport details.	2 years 3 months from the date on which the individual leaves Wasteland.	Legal requirement to retain information for this period (right to work information). We have added a cushion of 3 months in case of any issues raised by UK Visas and Immigration.
A member of staff's CV / education and training details / application to join Wasteland / references / health records / HR records.	6 years 6 months from the date on which the individual leaves Wasteland.	6 years is the limitation period within which to bring breach of contract / negligence claims. We have added a cushion of 6 months in case of litigation at the end of the period.
A member of staff's emergency contact information.	Destroy as soon as the individual leaves Wasteland.	No need to retain this information.
A member of staff's contact details not included in the documentation referred to above.	6 months from the date on which the individual leaves Wasteland.	Retain information for this period so we can contact them to deal with any hand-over issues.

Personal data (CV and contact details) relating to job applicants who we do not hire.	Destroy immediately or obtain explicit consent from the applicant for us to retain this information in case a suitable opportunity comes up for them in the future.	If an applicant is unsuitable there is no need to retain this information. If an applicant is impressive but we don't hire them we may want the opportunity of contacting them in future if a vacancy arises.
Personal data (CV and contact details) relating to individuals on work experience.	Destroy immediately or obtain explicit consent from the individual for us to retain this information in case a suitable opportunity comes up for them in the future.	If an individual on work experience is unsuitable there is no need to retain this information. If an individual on work experience is impressive but we don't hire them we may want the opportunity of contacting them in future if a vacancy arises.
Records that do not contain personal data.	Do not destroy unless you know that there is no business value in retaining them.	There is no legal requirement to minimise the storage of non-personal data.