RETENTION POLICY

OAKLAND SEARCH

Prepared by – DPAS

Date December 2025

Version One

TABLE OF CONTENTS

1. INTRODUCTION 2
2. SCOPE OF THIS POLICY 2
3. PURPOSE OF THIS POLICY 3
4. HOW TO DETERMINE THE LENGTH OF RETENTION? 3
5. BUSINESS REQUIREMENTS 4
6. STATUTORY AND REGULATORY REQUIREMENTS 5
7. WHO IS RESPONSIBLE FOR DATA RETENTION AND DISPOSAL? 5
8. WHAT DO ORGANISATIONS HAVE TO DO? 5
9. SETTING TRIGGER POINTS 5
10. DISPOSAL ACTION 6
11. SECURE DISPOSAL 6
12. REVIEW AND APPROVAL 6
DOCUMENT HISTORY AND VERSION CONTROL 7

1.INTRODUCTION

1.1 This policy applies Oakland Search which is a limited company registered in England and Wales under registration number12297897 with a registered office at 128 City Road, London, United Kingdom, EC1V 2NX. Oakland Search is the 'Controller' of any personal information it processes.

1.2 The UK General Data Protection Regulations (UK GDPR) principles require that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (Article 5 (1) (e) – Storage Limitation).

1.3 This means that if personal data is no longer in use or required to be kept for a specific purpose then you should either securely destroy it or anonymise all parts of the information that could give away the identity of the individual. By dealing with data in this way you are meeting the storage limitation principle in the UK GDPR.

1.4 As the controller of data, under Article 5(2) (accountability), we shall be responsible for and demonstrate compliance with the principles set out in Article 5 of the UK GDPR.

1.5 It is set out in multiple policies in accordance with Article 24, that Oakland Search will adhere to the data protection principles set out within the UK GDPR.

1.6 Personal data should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. It is explained in Recital 39 of the UK GDPR that this means ensuring the period for which the personal data are stored is limited to a strict minimum.

1.7 Failure to adhere to this policy could result in fines and penalties, along with damage to reputation.

2.SCOPE OF THIS POLICY

2.1 Oakland Search retains records in relation to its business, all employees, former employees, and clients.

2.2 This policy also applies to records that third parties process on behalf of Oakland Search for example, cloud storage providers or offsite records storage.

2.3 This policy applies to all staff and individuals who handle personal data on behalf of Oakland Search, whether employed on a full-time, part-time, temporary, or permanent basis, including contractors.

2.4 This policy has been developed to support a consistent organisation wide approach to the retention and disposal of personal data regardless of format, for example, paper or electronic, whether that's via emails or another method of online communication.

2.5 It sets out what Oakland Search needs to do to ensure that it is compliant with the data retention requirements of the UK GDPR.

2.6 The schedule covers personal data in respect of all data subjects (employees, former employees, clients, customers, candidates, employees, and intermediaries) which is collected, stored, and processed by Oakland Search.

2.7 This policy and its schedule apply to all records of personal data, be they stored electronically or in hard copy. It also applies to data that belongs to us, held by employees on personal devices.

2.8 The burden is placed upon Oakland Search to justify the necessity for retaining personal data once the specific purpose has ended. The reasons for retaining data must be identified on the data retention schedule.

3.PURPOSE OF THIS POLICY

3.1 Effective data retention and disposal procedures will ensure that Oakland Search will:

- Protect vital information, which it needs to function effectively.
- Reduce the risk of losing special category personal data and other sensitive personal information that could potentially cause harm to the individuals involved.
- Conform to any legal and statutory requirements.
- Dispose appropriately of information that is no longer required.
- Ensure a consistent approach is used in relation to the destruction of records that are not permanently required.
- Promote improved records management practices.

3.2 Disposing of personal data when no longer needed, will avoid exposure to risks around:

- **Efficiency:** Keeping too much information will impede the performance of digital systems and could make it difficult to find the information required to carry out business functions or to respond to a Data Subject Requests. It may also be hard to maintain large amounts of digital information and ensure that it is complete, available, and usable.
- **Cost:** There are significant costs around maintaining, preserving, and providing personal information to the data subject and the more information you hold the more expensive this will be. Also, not complying with data protection legislation can lead to significant financial penalties.
- **Reputation:** Not disposing of information in a responsible and timely fashion will put an organisation at risk of non-compliance with the requirements for storage limitation under the GDPR and, in the event of a data breach, the potential for a large fine and reputational damage will be much higher.

4.HOW TO DETERMINE THE LENGTH OF RETENTION?

4.1 It is not acceptable under UK GDPR to retain personal data indefinitely, unless explicitly required to by law.

4.2 Therefore, Oakland Search must assess what a reasonable period is to retain personal data beyond its original purpose and set this out in a transparent way. A link to Oakland Search's Retention Schedule should be included in any Privacy Notice to ensure that data subjects understand what is being done with their personal data.

4.3 Oakland Search must retain records which contain information that:

- Has enduring business value (for example, it provides a record of a business transaction, evidences its rights or obligations, protects its legal interests, or ensures operational continuity) (see Section 5 below).
- must be kept satisfying legal, accounting, or other regulatory requirements (see Section 6 below).

4.4 Oakland Search therefore prohibits the inappropriate destruction or retention of any records, files, documents, samples, and other forms of information. A retention schedule setting out Oakland Search's retention periods can be found [HERE].

4.5 The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for Oakland Search and/or its employees:

- Fines and penalties.
- Perversion of justice charges.
- Inference of destruction of evidence and other claims.
- Contempt of court charges.
- Serious disadvantages in litigation loss of rights.

5.BUSINESS REQUIREMENTS

5.1 If personal data has been recorded because of a contractual relationship (such as a client who Oakland Search no longer do business with), Oakland Search should keep some information beyond the end of the original purpose so that it can confirm that the relationship existed and that it has ended, and to enable it to deal with any complaints or claims which may arise in relation to the services provided. The retention period for this information should be appropriate and proportionate.

5.2 Personal data collected for prospective candidates will not be kept beyond 2 years, from the date the commutations ceased, unless so requested by the data subject.

5.3 Personal data that is held about an employee should be reviewed when their employment ends. Sufficient data will need to be retained to deal with future queries such as providing references or information about the individual's pension arrangements. However, personal data that is unlikely to be needed again, such as the individual's emergency contact details, previous addresses, or death-in-service beneficiary details, should be deleted.

6.STATUTORY AND REGULATORY REQUIREMENTS

Retention periods need to take account of any professional rules or regulatory requirements that apply. There are various legal requirements and professional guidelines about keeping certain kinds of records, such as information needed for income tax and audit purposes, or information on aspects of health and safety. Most of the data retention requirements for key regulators and directives that impact on Oakland Search are set out in the Retention Schedule. However, this list is subject to change, and we must ensure that we understand and apply the statutory and regulatory requirements for the personal data that we hold.

7.WHO IS RESPONSIBLE FOR DATA RETENTION AND DISPOSAL?

7.1 Oakland Search is responsible for maintaining its own Retention Schedule.

7.2 All staff are responsible for ensuring that retention and disposal of personal data is in line with the schedule for their business area.

7.3 At the end of the retention period, or the life of a particular record, it should be disposed of, unless there is an appropriate requirement for keeping it. Disposal does not necessarily mean destruction. It refers to the action taken at the end of the retention period and can include anonymization or secure deletion.

7.4 Staff should note that under the data protection legislation, it is a criminal offence to alter, deface, block, erase, destroy or conceal data which is the subject of a Subject Access Request (SAR) with the intention of preventing the disclosure of all or part of the information that the person making the SAR would have been entitled to receive. However, data may be amended or deleted after receipt of the SAR but before disclosure of the data, if the amendment or deletion would have taken place regardless of the SAR (e.g., under a Retention Schedule).

8.WHAT DO ORGANISATIONS HAVE TO DO?

A Retention Schedule is a list of types of records for which pre-determined Trigger Points, retention periods and disposal actions have been established. The Schedule should provide information on why records are retained for the length of time they are, how records should be disposed of, and any specific guidance for each type of record. Once created the schedule must be approved by the head of each business department.

9.SETTING TRIGGER POINTS

For each type of record an appropriate Trigger Point should be set. A Trigger Point is the date from which the data retention period starts. This is normally the end of the original purpose for the personal data. Common Trigger Points include date of birth, date of death, end of financial year, end of last action/use, or end of contract.

10. DISPOSAL ACTION

10.1 At the end of the retention period, or the life of a particular record, it should be disposed of, unless there is an appropriate requirement for keeping it. Disposal does not necessarily mean destruction. It refers to the action taken at the end of the retention period and can include anonymization or secure deletion.

10.2 It is important to keep a record of what was securely deleted, or otherwise disposed of, and when for audit purposes.

11. SECURE DISPOSAL

11.1 If it is appropriate to delete a record from a live system, it should also be securely deleted from any back-up of the information on that system.

11.2 **Hard copy:** Where paper files are to be disposed of internally or by external contractors confidential shredding protocols shall be adopted. Where external contractors are used there should be appropriate due diligence prior to the award of any contract and the contract should set out the confidential shredding protocols to be adopted and, as appropriate, require certification of destruction for audit purposes.

11.3 **Electronic:** Where electronic data is to be destroyed the protocols to be adopted should be put beyond use, shredded electronically, or deleted from all archived and live systems. Where such action is to be carried out by external contractors there should be appropriate due diligence prior to the award of any contract and the contract should set out the relevant destruction protocols to be adopted and, as appropriate, require a Certificate of Destruction for audit purposes.

11.4 The Information Commissioner's Office (ICO) will be satisfied that information has been 'put beyond use', even if is not actually deleted, provided that the data controller holding it:

- Is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way.
- Does not give any other organisation access to the personal data.
- Surrounds the personal data with appropriate technical and organisational security.
- Commits to permanent deletion of the information if, or when, this becomes possible.

11.5 The ICO will not require data controllers to grant individuals subject access to the personal data provided that all four safeguards above are in place. Nor will the ICO take any action for non-compliance with the data protection principle of storage limitation.

12. REVIEW AND APPROVAL

This policy does not form part of any employment contract and is subject to change at any time and will be updated from time to time to reflect best practice and changes in legislation.
This policy will be reviewed every 12 months, or earlier, should this be required to suit the needs of the business and meet statutory requirements.

DOCUMENT HISTORY AND VERSION CONTROL

Version No.	Author	Effective Date	Status/Comments
V0.1	Kristal Rocks	09.03.2026	

REVIEW AND APPROVAL

This policy will be reviewed regularly and may be altered from time to time in light of legislative changes or other prevailing circumstances.

Reviewer	Job Title	Signed Off Date	Status/Comments

Next Review Date
All policies should be reviewed at least annually or when significant change occurs to the policy subject matter. The next review date for this policy is **30.03.2027.**