THE RECRUITMENT Co

Data Retention Policy (UK).

CONTENTS

CLAUSE

ANNEX

1. ABOUT THIS POLICY

1.1 The corporate information, records and data of Twenty20 Capital Bidco1 Limited and our subsidiaries is important to how we conduct business and manage employees.

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 Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 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 data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. 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.

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

2.4 This policy applies to the following Twenty20 Capital Bidco1 LImited group companies in the United Kingdom (and a reference to "**we**", "**us**", "**our**", "**Supplier**", "**Agency**" or "**Twenty20**" shall mean the specific company which is delivering services (including any trading or brand name of that underlying legal entity):

> The UK Recruitment Co. Limited trading as The Recruitment Co, Staffgroup International Limited, Earthstaff Limited, Staffgroup Limited, Staffgroup GmbH, Staffgroup Engineering GmbH and Staffgroup SAS.

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 Legal Department. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee'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 Each of the Twenty20 companies is responsible for identifying the data that we must or should retain, and determining, in collaboration with the Data Protection Manager (DPM), the proper period of retention. It also arranges for the proper storage and retrieval of data, coordinating with outside vendors where appropriate.

4.3 Each of the Twenty20 companies is responsible for:

- Administering the data management programme;
- Helping department 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.

4.4 **Data Protection Manager.** Our Data Protection Manager (DPM) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. Our DPM works with our senior leaders on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

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.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Twenty20 and retained primarily for reference purposes.
- 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.

Confidential information belonging to others. Any confidential information that an employee may have obtained from a source outside Twenty20, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

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 business 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 DPM.

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 DPM.

7. STORAGE, BACK-UP AND DISPOSAL OF DATA

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

7.2 **Destruction**. Each of the Twenty20 Capital Bidco1 Limited group companies is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be coordinated with the IT Department.

7.3 The destruction of data must stop immediately upon notification from the Legal Department that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Legal Department lifts the requirement for preservation.

8. SPECIAL CIRCUMSTANCES

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Record Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Legal Department informs you, 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 Legal Department 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.

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

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

9.1 **Questions about the policy.** Any questions about retention periods relevant to your department should be raised with your department manager. Any questions about this policy should be referred to the DPM, 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, depends largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the DPM. If employees 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**. Our DPM will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice] to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

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, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

Data Protection Manager: our Data Protection Manager is responsible for advising on and monitoring compliance with data protection laws.

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.

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

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.

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 UK GDPR as the principle of storage limitation.

ANNEX B RECORD RETENTION SCHEDULE

Establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with the Data Retention Policy.

If you hold data not listed below, please refer to the Data Retention Policy. 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 the DPM.

Type	Personal Information To Delete	Retention Period
Worker Seeker	Right to Work & Bank Account information	6 months from registration
Worker Seeker	All information excluding Right to Work & Bank Account information	12 months from registration
Worker (individual who has worked for the company)	All information excluding medical records & pension information	7 years after employment has ceases

Data record types with statutory retention periods

Accident books, accident records/reports
Statutory retention period: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos).
Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

Accounting records
Statutory retention period: 6 years for public limited companies.
Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

Income tax and NI returns, income tax records and correspondence with HMRC
Statutory retention period: not less than 3 years after the end of the financial year to which they relate.

Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

Medical records and details of biological tests under the Control of Lead at Work Regulations
Statutory retention period: 40 years from the date of the last entry.
Statutory authority: The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)
Statutory retention period: 40 years from the date of the last entry.
Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates
Statutory retention period: (medical records) 40 years from the date of the last entry; (medical examination certificates) 4 years from the date of issue.
Statutory authority: The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)

Medical records under the Ionising Radiations Regulations 1999
Statutory retention period: until the person reaches 75 years of age, but in any event for at least 50 years.
Statutory authority: The Ionising Radiations Regulations 1999 (SI 1999/3232).

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)
Statutory retention period: 5 years from the date on which the tests were carried out.
Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

Records relating to children and young adults
Statutory retention period: until the child/young adult reaches the age of 21.
Statutory authority: Limitation Act 1980.

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity
Statutory retention period: 6 years from the end of the scheme year in which the event took place.
Statutory authority: The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence
Statutory retention period: 3 years after the end of the tax year in which the maternity period ends.
Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.

Wage/salary records (also overtime, bonuses, expenses)
Statutory retention period: 6 years.
Statutory authority: Taxes Management Act 1970.

National minimum wage records
Statutory retention period: 3 years after the end of the pay reference period following the one that the records cover.
Statutory authority: National Minimum Wage Act 1998.

Records relating to working time
Statutory retention period: 2 years from date on which they were made.
Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

Work-seeker records
Statutory retention period: one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.
Statutory authority: The Conduct of Employment Agencies and Employment Businesses Regulations 2003 and The Gangmasters (Licensing Conditions) Rules 2009

Records relating to dealings with other licence holders
Statutory retention period: one year from creation or, where they have been supplied by another person, from last supply.
Statutory authority: The Gangmasters (Licensing Conditions) Rules 2009

Data Record types with non-statutory retention periods

Actuarial valuation reports
Retention period: permanently.

Application forms and interview notes (for unsuccessful candidates)
Retention period: One year.

Assessments under health and safety regulations and records of consultations with safety representatives and committees
Retention period: permanently.

Inland Revenue/HMRC approvals
Retention period: permanently.

Money purchase details
Retention period: 6 years after transfer or value taken.

Parental leave
Retention period: 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.

Pension scheme investment policies
Retention period: 12 years from the ending of any benefit payable under the policy.

Pensioners' records
Retention period: 12 years after benefit ceases.

Personnel files and training records (including disciplinary records and working time records)
Retention period: 6 years after employment ceases.

Redundancy details, calculations of payments, refunds, notification to the Secretary of State
Retention period: 6 years from the date of redundancy

Senior executives' records (that is, those on a senior management team or their equivalents)
Retention period: permanently for historical purposes.

Statutory Sick Pay records, calculations, certificates, self-certificates
Retention period: The 6 years after the employment ceases.

Trade union agreements
Retention period: 10 years after ceasing to be effective.

Trust deeds and rules
Retention period: permanently.

Trustees' minute books
Retention period: permanently.

Works council minutes
Retention period: permanently.