DATA RETENTION AND DESTRUCTION POLICY

1. ABOUT THIS DATA PROTECTION AND DESTRUCTION POLICY

1.1 Fygo Technologies Limited of Kemp House, 160 City Road, London EC1V 2NX, UK ("**Fygo**" or "**us**" or "**we**"), are committed to protecting data. In operating and maintaining the Fygo mobile application ("**Fygo App**"), Fygo collects the data of users and employees.

1.2 This Data Retention and Destruction Policy sets out how (and for how long) Fygo stores, and eventually destroys data. There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time.

1.3 This Data Retention and Destruction Policy explains Fygo's requirements to retain data and to dispose of data and provides directions for the appropriate handling and disposal of data. This policy also informs Fygo employees of their roles and responsibilities in relation to the personal data held by Fygo.

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.

1.6 This policy has been prepared with due regard to the General Data Protection Regulation (EU Regulation 2016/679) ("**GDPR**").

1.7 For further information on Fygo's collection and handling of personal data, please refer to Fygo's Cookie Policy and Privacy Policy, which are available on our website at https://www.fygo.co/legals/ (the "**Fygo Website**").

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. It also covers data that belongs to us but is held by employees on personal devices in accordance with our Bring Your Own Device (BYOD) Policy.

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 all business units and functions of Fygo.

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

Data Retention and Destruction 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.
Records Management Officer:	the Records Management Officer is head of the Records Management Department and is responsible for administering the data management programme, helping department heads implement it 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.
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 GDPR as the principle of storage limitation.

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 contained within it, any communications suspending data disposal and any specific instructions from Fygo, particularly the Records Management Officer. Failure to do so may subject Fygo, our employees, and/or 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 Records Management Officer. The Records Management Officer is responsible for identifying the data that Fygo must or should retain and determining the proper period of retention. They also arrange for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate. Additionally, the Records Management Officer handles the destruction of some records whose retention period has expired.

4.3 The Records Management Officer is responsible for:

(a) Administering the data management programme;

(b) Helping department heads implement the data management programme and related best practices;

(c) Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and

(d) Providing guidance, training, monitoring, and updating 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:

(a) Duplicates of originals that have not been annotated;

(b) 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;

(c) Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Fygo and retained primarily for reference purposes; and

(d) 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. Personal data is contained in structured records (such as databases) and unstructured records (such as documents and spreadsheets), in emails, in audio and video recordings and includes personal data we generate (such as through access control systems and in personnel files) as well as personal data provided to us. 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.

5.4 Confidential information belonging to others. Any confidential information that an employee may have obtained from a source outside of Fygo, 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 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 Records Management Officer.

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 if it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of. For guidance on how to make decisions on how long to retain disposable information, please contact the Records Management Officer.

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 considered the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must consider the principle of storage limitation when deciding whether to retain this data. For guidance on how to make decisions on how long to retain disposable information, please contact the Records Management Officer. In certain situations, personal data may be kept for longer than as set out in the Record Retention Schedule, but only where the DPO has given their approval and where Fygo has reasonable grounds for retaining the personal data beyond the retention period. Examples include situations where:

(a) the personal data is required for the exercise or defence of legal claims, and appropriate technical and organisational measures have been applied to the continued retention of the personal data to protect the risks to rights and freedoms of the data subjects;

(b) the personal data is required by Fygo for statistical purposes and appropriate safeguards (pursuant to Article 89(1) of the GDPR) have been applied to the processing for these purposes, to protect the risks to rights and freedoms of data subjects;

(c) the personal data has been fully and effectively anonymised and the DPO is satisfied that data subjects cannot be identified from the anonymised data.

When the Records Management Officer is establishing or reviewing personal data retention periods, the following shall be considered:

(a) the lawful basis upon which the personal data is collected and processed;

(b) whether the personal data is special category personal data or relates to criminal convictions or offences;

(c) the risk to rights and freedoms of data subjects associated with collecting, holding, and processing the personal data;

(d) Fygo's legal or regulatory obligations to collect or retain the personal data in question; and

(e) Fygo's objectives and requirements when collecting and processing the personal 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 Records Management Officer.

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 (general). Our Records Management Officer 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.

7.3 Destruction (personal data). Personal data shall be disposed of, where this is technically possible, in the following circumstances:

(a) on expiry of the retention period set out in the Record Retention Schedule;

(b) in response to a request from a data subject to erase their personal data where the Fygo Subjects Rights Procedure has been followed and the Data Protection Officer has confirmed the personal data should be destroyed; and

(c) at the discretion of a Fygo Director where retention of the personal data is no longer necessary for the purpose of the processing prior to the expiry of the relevant retention period, and the Data Protection Officer has confirmed the personal data should be destroyed.

Where personal data is erased at the request of a data subject, Fygo may retain such limited personal data as is reasonably necessary to keep a record of the erasure for the purposes of demonstrating compliance, and enforcing erasure across all business systems, provided appropriate technical and organisational measures have been applied to the retained data in order to protect the risks to rights and freedoms of the data subject.

The personal data which may be erased, destroyed, or otherwise disposed of in a secure manner, is as follows:

(a) personal data held in electronic records (including back-ups);

(b) personal data held in physical records (including archives) which must be crosscut shredded as 'confidential waste'; and

(c) special category or other sensitive personal data held in physical records (including archives) which must be crosscut shredded as 'confidential waste'.

In all cases, proof of destruction is to be recorded. Where an external destruction supplier is used, a certificate of destruction must be provided by the supplier.

Electronic or physical records may contain different types of personal data which are used for different purposes. These different types of personal data may be subject to different retention periods or have different levels of sensitivity. It is therefore imperative that data itself is managed individually according to categories and not the physical or electronic file as a whole. It may be necessary to destroy some data from a file, at the same time retaining other information from the same file.

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 if Fygo 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 Fygo 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 Records Management Officer.

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. BREACH REPORTING AND AUDIT

9.1 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 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 Records Management Officer. 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.

9.2 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.

9.3 Audits. The Records Management Officer will periodically review this policy and its procedures including where appropriate by taking outside legal or auditor advice to ensure we comply with relevant new or amended laws, regulations, or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

RECORD RETENTION SCHEDULE

Fygo 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.

If you are an employee and you hold data not listed below, 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 Records Management Officer.

Category of personal data	Retention period	Rationale for retention period
Service user contact details	Trigger: upon voluntary termination of the service, graduation or ceasing employment with higher education establishment. Maximum: 2 years	If consent was the lawful basis for processing the data, that consent may be withdrawn at any time. If user accounts remain dormant for a continuous period of two years, all personal data (excluding financial transaction data) shall be destroyed.
Service user financial transaction details	Trigger: upon voluntary termination of the service, graduation or ceasing employment with higher education establishment. Maximum: 13 months from date of a transaction	Contractual relationship with card-linking third-party service provider.
HR files other than as specified below	Trigger: termination of employment. Maximum: 8 years	7-year period advisable as a claim in relation to a person's employment could be a breach of contract claim.
Payroll and wage records (including summaries of expenses, payment made on the employee's behalf)	Trigger: end of accounting period. Maximum: 8 years	Compliance with tax legislation.
Job applications and interview records of unsuccessful candidates. This includes unsolicited job applications and CVs	Trigger: notification the candidate was unsuccessful. Maximum: 1 year	An Employment Tribunal case must be brought within 3 months. The longer periods account for the fact that a tribunal has quite a wide discretion to extend the time period when it is "just and equitable to do so". Once deleted personal info is anonymised for statistical analysis.
Accident reports and records, accident record books, health and safety policy, assessments	Trigger: record created. Maximum 45 years	Records which deal with assessments of health and safety risks and steps taken to reduce or prevent them should be kept until the regulations they obey

		are superseded or are no longer relevant. However, it is advisable to keep all records relating to health and safety standards for at least 40 years in line with the Control of Substances Hazardous to Health Regulations (COSHH)
Employees' Pension Scheme Documentation	Trigger: date of record. Maximum: N/A	As there are no time limits in relation to when certain actions may be brought by beneficiaries
Immigration / right to work checks	Trigger: termination of employment / contract. Maximum: 3 years	Compliance with the Immigration, Asylum and Nationality Act 2006
Statutory Maternity Pay Records, calculations, certificates (Mat B1s) or other medical evidence	Trigger: last day of statutory maternity leave. Maximum: 4 years	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Subject Access Requests (SAR) – including information compiled for the purposes of meeting the request	Trigger: date of last action related to the SAR. Maximum: 2 years	To permit requestors to make any necessary appeals
Tax returns and associated computations, signed statements, report and accounts, auditor's reports. Accounting records, including all supporting documentation such as cashbooks, petty cash books, etc. - VAT records - Corporation tax records	Trigger: end of accounting period. Maximum: 8 years	Takes account of HMRC requirements that such documents should be kept for 6 years from the end of the accounting period to which they relate (Section 388 Companies Act 2006 and, for VAT, HMRC Notice 700/21)