Rapid IT

Data Processing Agreement and T&C's

(Main Contract)

APPROVAL AND VERSION CONTROL

Version:	13	Implemented:	10.10.24	Next Review Date:	10.10.2025

DATA PROCESSING CONTRACT

BETWEEN:

(1) _____

with registered office at _____

(hereinafter referred to as **"[CONTROLLER]**");

and

(2) **RAPID IT RECYCLING LIMITED** incorporated in 2010 with registered office at Tech Warehouse, Wyre Street, Padiham, Lancashire, BB12 8DF (hereinafter referred to as the **"[PROCESSOR]")**.

WHEREAS:

(A). **[CONTROLLER]** wishes to appoint **[PROCESSOR]** to undertake the Services (as defined in Schedule 4) on its behalf.

(B). To perform the Services on **[CONTROLLER]**'s behalf, **[PROCESSOR]** will require to process certain Categories of Data (as defined in the DIAL rating) on behalf of **[CONTROLLER]**.

(C). The Parties now wish to enter into this Contract (as defined below) to regulate the processing of these Categories of Data by **[PROCESSOR]** on behalf of **[CONTROLLER]**.

IT IS HEREBY AGREED:

1. Definitions and Interpretation

1.1 The words and expressions below will have the meanings set out next to them:

"Applicable Laws" means any other law or regulation that may apply to the processing of Personal Data;

"Appointed Agent" means any auditor or third party, formally appointed by the Data Controller to perform a range of tasks associated with the validation of the performance of the Data Processor.

"Confidential Information" means all confidential information imparted by **[CONTROLLER]** to **[PROCESSOR]** during the term of this Contract or coming into existence because of **[PROCESSOR]**'s obligations hereunder which is either marked as confidential or which ought reasonably be regarded as confidential;

"Contract" means this Data Processing Contract;

"Controller Data" means all data processed by the Data Processor on behalf of the Data Controller under the terms of this data processing contract.

"Data Controller" means "controller" as defined in Article 4 (7) of the GDPR;

"Data Processor" means "processor" as defined in Article 4 (8) of the GDPR;

"Data Subject" means "data subject" as defined in Article 4 (1) of the GDPR

"GDPR" means the General Data Protection Regulation Directive 2016/679;

"Personal Data" means "personal data" as defined by Article 4 (1) of the GDPR and which is processed by **[PROCESSOR] on** behalf of **[CONTROLLER]**, as set out in Schedule 4 hereto;

"Party" or "Parties" means a party or the parties to this Contract;

"Services" means the provision of various services including collection, sanitisation, recycling, disposal and relocation of IT Equipment to **[CONTROLLER]** deemed to be the subject matter as per Article 28 GDPR;

"Data Subject Rights Request" means a request under Chapter 3 of GDPR which relates to the processing of Personal Data by **[PROCESSOR]** on behalf of **[CONTROLLER]**; and

"Third Party" means a party which is not [**CONTROLLER]**, **[PROCESSOR]** or the Data Subject to whom the Personal Data relates.

1.2 In this Contract unless otherwise expressly stated:

1.1.1. references to Clauses are to clauses of this Contract;

1.1.2. reference to the Schedules are to the schedules to this Contract which form part of this Contract and are incorporated herein;

1.1.3. references to the singular include references to the plural and vice versa;

1.1.4. headings are inserted for convenience only and shall not affect the construction or interpretation of this Contract;

1.1.5. any phrase introduced by the terms "including", "include", "in particular" or any similar expression are illustrative and do not limit the sense of the words preceding those terms and such terms shall be deemed to be followed by the words "without limitation";

1.1.6. references to a statute, or any section of any statute, include any statutory amendment, modification or re-enactment and instruments and regulations under it in force from time to time;

1.1.7. references to regulatory rules include any amendments or revisions to such rules from time to time; and

1.1.8. references to regulatory authorities refer to any successor regulatory authorities.

2. Subject and scope of the commissioned processing of Personal Data

2.1 **[PROCESSOR]** processes the Controller Data exclusively on behalf of and on the instruction of **[CONTROLLER]** in accordance with Article 28 (1) GDPR (Commissioned Data Processing). **[CONTROLLER]** remains the controller for the purposes of data protection law.

2.2 The Customer's DIAL rating (risk assessment) forms part of this contract and includes a list of types of Controller Data the Processor may process, the nature and purpose of processing and to which categories of data subjects the Controller Data relate as per Article 28 (3).

2.3 In the absence of a written customer specification, the maximum length of time from the point of collection until the point of data sanitisation shall be done as soon as possible but no longer than 45 working days for a DIAL 1 rating and 20 working days for a DIAL 2 rating.

2.4 The processing of Controller Data will take place exclusively within the territory of the United Kingdom. Data processing in other countries may only take place where the [CONTROLLER] has provided their prior written consent and, where applicable, additionally the requirements of Article. 44 to 47 GDPR are fulfilled, or there is an exception in accordance with Article 49 GDPR.

3. Standards of Performance

3.1. **[PROCESSOR]** hereby undertakes to **[CONTROLLER]** that it will undertake the Services on behalf of **[CONTROLLER]** in accordance with this Contract using all reasonable skill and care.

3.2. **[PROCESSOR]** hereby provides sufficient guarantees to implement appropriate technical and organisation measures in such a manner that processing meets the requirements of Article 28 (1) of GDPR. These guarantees are listed in Schedule 5.

3.3. **[CONTROLLER]** and **[PROCESSOR]** hereby acknowledge that in relation to the Personal Data and for the purposes of the Applicable Laws, **[CONTROLLER]** is the Data Controller and **[PROCESSOR]** is the Data Processor.

4. The Term

4.1 This Contract shall continue in full force unless or until terminated in pursuance of Clause 19.

5. Obligations of [CONTROLLER]

5.1. **[CONTROLLER]** shall provide such information as **[PROCESSOR]** may reasonably require for **[PROCESSOR]** to provide the Services outlined in Schedule 4. For amendment

5.2. **[CONTROLLER]** shall instruct **[PROCESSOR]** generally in written or text form which includes email communication. If required, **[CONTROLLER]** may also issue instructions orally or via telephone. Instructions issued orally or via telephone require, however, immediate confirmation by **[CONTROLLER]** in written or text form.

5.3. **[CONTROLLER)** shall have legal title on all goods being collected and therefore can instruct **[PROCESSOR]** to process equipment in accordance with the service agreed in the schedule laid out in this contract.

6. Obligations of [PROCESSOR]

6.1. **[PROCESSOR]** undertakes to **[CONTROLLER]** that it shall process the Personal Data only on **[CONTROLLER]**'s instructions as given from time to time, and in accordance with the terms of this Contract and all Applicable Laws.

6.2. Any instructions issued by **[CONTROLLER]** to **[PROCESSOR]** shall be done so in accordance with 5.2 and shall be documented by **[PROCESSOR]** to be evidenced to **[CONTROLLER]** on request.

6.3. If **[PROCESSOR]** is of the reasonable opinion that an instruction by **[CONTROLLER]** breaches this Agreement, an earlier instruction, or applicable data protection laws**,** **[PROCESSOR]** must inform **[CONTROLLER]** in writing of this immediately.

6.4. **[PROCESSOR]** shall ensure that only such of its employees who may be required by **[PROCESSOR]** to assist it in meeting its obligations under this Contract shall have access to the Personal Data. **[PROCESSOR]** shall ensure that all employees used by it to provide the Services (i) have undergone training in the laws of data protection and in the care and handling of the Personal Data in accordance with such laws, and (ii) have undergone vetting to an appropriate level.

6.5. In particular, **[PROCESSOR]** undertakes to **[CONTROLLER]** that it will not disclose the Personal Data or any part thereof to any Third Party unless and only to the extent instructed to do so in writing by **[CONTROLLER].**

6.6. **[PROCESSOR]** undertakes to **[CONTROLLER] that** it will not export the Personal Data or any part thereof outside the United Kingdom in any circumstances other than at the specific written request of **[CONTROLLER**]. If **[PROCESSOR]** intends to transfer Controller Data to a third country or an international organisation without having been instructed to this end by **[CONTROLLER], [PROCESSOR]** will inform **[CONTROLLER]** without undue delay and as soon as possible about the purpose, legal ground and affected Controller Data, to such an extent and insofar as such notification is not legally prohibited on the grounds of a substantial public interest.

6.7. For the mutual benefit of both Parties, and to ensure compliance with this Contract and the Applicable Laws, **[CONTROLLER]** and **[PROCESSOR]** will liaise regularly, and **[PROCESSOR]** will allow its data processing facilities, procedures and documentation to be reviewed by **[CONTROLLER]** or its auditors.

6.8. If at any time **[PROCESSOR]** is unable to meet any of its obligations under this Contract, it undertakes to inform **[CONTROLLER]** immediately by notice in writing.

6.9. **[PROCESSOR]** is not permitted to make any copies or duplicates of the Controller Data without prior written approval by **[CONTROLLER].**

6.10. Should **[CONTROLLER]** be required to provide information to a public authority or a person relating to the processing of Controller Data, or to otherwise cooperate with a public authority, **[PROCESSOR]** shall support **[CONTROLLER]** at the first request with the provision of such information or the fulfilment of other obligations to cooperate. This applies to immediate provision of all information and documents relating to technical and organisational measures taken in line with Article. 32 GDPR relating to the technical procedure for the processing of Controller Data, the sites at which Controller Data are processed, and relating to the employees involved in processing the Controller Data

6.11. **[PROCESSOR]** will support **[CONTROLLER]** in any activity, relevant to services being carried out by **[PROCESSOR],** which **[CONTROLLER]** or appointed agents must undertake to comply with GDPR such as Data Privacy Impact Assessment and Register of Processing Activities.

6.12. **[PROCESSOR]** must have a Data Protection Officer throughout the term of this contract and inform **[CONTROLLER]** of the contact details of this appointment. Should the **[PROCESSOR]** make any changes to the Data Protection Officer this information must be passed onto **[CONTROLLER]** without undue delay. Should **[PROCESSOR]** believe they do not have to appoint a Data Protection Officer this information should be passed onto **[CONTROLLER]** prior to the enactment of this contract.

7. Assignment & Subcontracting

7.1. **[PROCESSOR]** shall not be entitled to assign this Contract nor all or any of its rights or obligations hereunder, without the prior written consent of **[CONTROLLER]**.

7.2. The **[CONTROLLER]** hereby consents to the use by the **[PROCESSOR]** of the services of the subcontractors set out in Schedule 3of this Agreement for the purposes set out therein.

7.3. **[PROCESSOR]** shall not be entitled to sub-contract performance of its obligations hereunder without **[CONTROLLER]**'s prior written consent and **[PROCESSOR]** shall, at all times, be responsible as between itself and **[CONTROLLER]** for the observance by its assignees of the obligations contained in this Contract as if such sub-contractors were **[PROCESSOR].**

7.4. In the event that **[PROCESSOR]** requires **[CONTROLLER]**'s prior written consent in pursuance of Clause 7, **[CONTROLLER]** shall be entitled, at its discretion, to withhold such consent and prior to issuing such consent **[CONTROLLER]** may require the party that **[PROCESSOR]** proposes to sub-contract the performance (or any part thereof) of its obligations hereunder, to enter into a direct contractual relationship with **[CONTROLLER]** in respect of the processing of any Personal Data by such party.

7.5 For the assessment of such approval, **[PROCESSOR]** must provide **[CONTROLLER]** with a copy of the intended commissioned data processing agreement between **[PROCESSOR]** and the further commissioned data processor. **[PROCESSOR]** must obligate the further commissioned data processor in that written agreement in exactly the same manner as the former is obligated on the basis of this Agreement and include the requirements set out in Clause 14.

7.6 **[PROCESSOR]** is obligated to only select – and, should **[CONTROLLER]** approve, to make use of – those further commissioned data processors which offer sufficient guarantees that the appropriate technical and organisational measures will be implemented in such a manner that the processing of Controller Data takes place in accordance with the requirements of the GDPR. **[PROCESSOR]** must satisfy itself prior to the commencement of the processing of compliance with the technical and organisational measures by the further commissioned data processor and will confirm by means of a request for approval by **[CONTROLLER]**. Upon request, **[PROCESSOR]** will provide evidence to **[CONTROLLER]** to this end.

7.7 There is no right or claim to the granting of approval. The statutory liability of **[PROCESSOR]** in their capacity as commissioned data processor remains unaffected by any approval granted.

7.8 **[CONTROLLER]** must also be granted audit and examination rights in relation to subcontractors in accordance with Clause 6 of this Contract. **[CONTROLLER]** may request from **[PROCESSOR]** information about the essential terms and conditions of the subcontract and the implementation of the subcontractor's obligations relating to data protection, if necessary, also by inspection of the relevant contractual documentation.

8 Security of processing (As per Article 32 GDPR)

8.1 **[PROCESSOR]** warrants that it undertakes appropriate technical and organisational measures to ensure a suitable level of protection for the Controller Data corresponding to the risk. This must be in consideration of the state of the art, implementation costs and the type, scope, circumstances, and aims of the processing as well as the varying likelihood of occurrence and severity of the risk to the rights and freedoms of data subjects. These measures include, *inter alia*, the following:

a) the pseudonymisation and encryption of Controller Data;

b) the ability to permanently ensure the confidentiality, integrity and availability of the systems, services and Controller Data in connection with the processing;

c) the ability to rapidly recover the availability of the Controller Data and access to them, should a physical or technical disruption occur;

d) a process for the regular review, assessment, evaluation and evidence of the effectiveness of the technical and organisational measures for the purposes of ensuring the security of the processing.

8.2 **[PROCESSOR]** guarantees that it has, prior to the commencement of the processing of the Controller Data, provided evidence to **[CONTROLLER]** that it has taken the appropriate technical and organisational measures to protect the data which is being processed. This evidence could be the accreditation of its Data Processing Service by an industry recognised accreditation scheme. (Article 28 (5) GDPR) **[PROCESSOR]** guarantees that it ill maintain these during the term of the Agreement.

8.3 **[PROCESSOR]** guarantees that it adheres to an approved code of conduct [Article 28 (5)] prior to the commencement of the contract.

8.4 **[PROCESSOR]** guarantees that as technology and threat evolves, by means of continual assessment, the technical and organisational measures in place are assessed for appropriateness. Because of this assessment **[PROCESSOR]** is permitted to implement alternative, adequate measures, if they do not fall below the security level of the measures agreed at the start of this Agreement. Any alternative measures are subject to the prior clauses of this contract and evidenced to **[CONTROLLER]** as per 8.1 and 8.2.

9. Transfer of Personal Data

9.1. Before transferring any Personal Data to **[CONTROLLER]**, **[PROCESSOR]** will establish with **[CONTROLLER]** the appropriate method of transfer or transmission and will securely transfer or transmit the Personal Data to **[CONTROLLER]** in line with **[CONTROLLER]**'s requirements.

10. Data Subject Requests

10.1. **[CONTROLLER]** shall be responsible for responding to all Data Subject Requests in accordance with Article 12. GDPR ("data subject rights") which may be received from Data Subjects to which the Personal Data relates.

10.2. **[PROCESSOR]** hereby agrees to assist **[CONTROLLER]** with all applicable Data Subject Requests which may be received from the Data Subjects to which the Personal Data relates as per Schedule 1.

10.3. If **[PROCESSOR]** receives a Data Subject Request from a Data Subject relating to the Personal Data processed on behalf of the **[CONTROLLER]** it shall immediately and without undue delay, forward it to the person nominated by **[CONTROLLER]** under clause 20 of this Contract.

10.4. Where **[CONTROLLER]** considers that it is necessary for copies of the Personal Data to be transferred to it to respond to a Data Subject Request, **[CONTROLLER]** will inform **[PROCESSOR]** that it requires copies to be transferred. Before transferring the copies, **[PROCESSOR]** will establish with **[CONTROLLER]** the appropriate method of transfer and will securely transfer the copies of the Personal Data to **[CONTROLLER]** in line with **[CONTROLLER]**'s requirements, to arrive no more than 10 working days from the date of **[CONTROLLER]**'s request to **[PROCESSOR]**.

11. Complaints relating to processing of Personal Data under this Contract

11.1. **[CONTROLLER]** shall be responsible for the handling of and responding to processing any complaints or expressions of dissatisfaction which may be received from the Data Subjects to which the Personal Data relates or others, in relation to the processing of the Personal Data under this Contract.

11.2. **[PROCESSOR]** hereby agrees to assist **[CONTROLLER]** with any applicable complaints or expressions of dissatisfaction which may be received from the Data Subjects to which the Personal Data relates or others, in relation to the processing of the Personal Data under this Contract as per Schedule 1

11.3. If [PROCESSOR] receives any complaints or expressions of dissatisfaction, relating to the Personal Data processed on behalf of the [CONTROLLER] it shall immediately and without undue delay, forward it to the person nominated by [CONTROLLER] under clause 20 of this Contract.

11.4. Where **[CONTROLLER]** considers that it is necessary for copies of the Personal Data to be transferred to it to allow it to respond to a complaint or expression of dissatisfaction, **[[CONTROLLER]** will inform **[PROCESSOR]** that it requires copies to be transferred. Before transferring the copies, **[PROCESSOR]** will establish with **[CONTROLLER]** the appropriate method of transfer and will securely transfer the copies of the Personal Data to **[CONTROLLER]** in line with **[CONTROLLER]**'s requirements, to arrive no more than 5 working days from the date of **[CONTROLLER]**'s request to **[PROCESSOR]**.

12. Breach Identification and Notification

12.1. Under the context of this contract a Data Breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

12.2.**[PROCESSOR]** will ensure that there are sufficient checks being made on processing activities to ensure that data is being protected at all times as per clause 8.

12.3. **[PROCESSOR**] will without undue delay inform **[CONTROLLER]** if the former becomes aware of an incident which under the definition of 12.1, constitutes a data breach. This communication will be made to the contact as designated in Clause 20 and be classed as "Initial Notification".

12.4. **[CONTROLLER]** will be responsible for informing the Local Supervisory Authority as denoted in Clause 20. This notification will be made no later than 72 hours from the "Initial Notification' as per Article 33 GDPR.

12.5. **[PROCESSOR]** must inform **[CONTROLLER]** within 24 hours of Initial Notification the following details where possible; natural of personal breach including categories and approximate number of data subjects concerned, names and contact details of the Data Protection Office or other contact point, likely consequences of personal data breach and any measures taken or proposed to be taken to mitigate the adverse effects of the data breach. Where it is not possible to provide this information in full within 24 hours, a clearly articulated plan of activities and timelines for obtaining any missing information should be submitted to **[CONTROLLER]** within the 24-hour window.

12.6. **[PROCESSOR]** will support the **[CONTROLLER]** or **[CONTROLLER]**'s appointed agent, in the investigation of any data breach incident unless such activities contravene legal or contractual obligations already in place. In such situations, a written explanation supporting the **[PROCESSOR]**'s position is required.

13. Retention and Disposal of Personal Data

13.1.**[PROCESSOR]** undertakes to retain and dispose of the Personal Data in line with the Retention and Disposal Guidelines, as contained in Schedule 6 to this Contract.

14. Evidence and inspections

14.1.**[PROCESSOR]** shall provide **[CONTROLLER]** with all necessary information to prove compliance with **[CONTROLLER**]'s obligations under this Agreement upon request. Upon request of **[CONTROLLER]**, **[PROCESSOR]** shall **provide [CONTROLLER]** immediately with all relevant certificates and audit reports.

14.2. **[CONTROLLER]** is entitled to receive information from the Data Protection Officer of **[PROCESSOR]** relating to all aspects regarding the processing of Controller Data, including the technical and organisational measures taken in accordance with Clause 8.

14.3. **[CONTROLLER]** or appointed agent is entitled, with reasonable notice, to enter the business premises of **[PROCESSOR]** during normal business hours (Mondays to Fridays from 09:00 until 18:00) and inspect the technical and organisational measures as well as the processes of **[PROCESSOR]**, to satisfy themselves of the compliance with the provisions of this Agreement as well as the relevant statutory data protection provisions by **[PROCESSOR]**.

14.4. **[PROCESSOR]** guarantees **[CONTROLLER],** or appointed agent, the access rights, information rights, and inspection rights necessary for this purpose. **[PROCESSOR]** will guarantee access to the data processing facilities, files, and other documents to allow for monitoring and auditing of the relevant data processing facilities, files and other documentation relating to the processing of the Controller Data. **[PROCESSOR]** will provide **[CONTROLLER]**, or an agent appointed by the same, with all information necessary for the inspection.

14.5. **[CONTROLLER]** and **[PROCESSOR]** are subject to public audits by the competent data protection authorities. Upon request of **[CONTROLLER]**, **[PROCESSOR]** will provide the requested information to the supervisory authorities and will also grant the latter the opportunity to audit; this includes inspections of **[PROCESSOR]** by the supervisory authorities and persons appointed by them. **[PROCESSOR]** guarantees to the competent authorities in this context the necessary access rights, information rights, and inspection rights.

14.6. **[PROCESSOR]** shall hold relevant industry accreditations to evidence capabilities in their field. These are to be maintained throughout the duration of this contract and are listed in Schedule 7**.**

15. Indemnity

15.1. **[PROCESSOR]** hereby agrees to indemnify **[CONTROLLER]** up to a maximum of £1million per incident against all losses, costs, expenses, damages, liabilities, demands, claims, fines, penalties, actions or proceedings which **[CONTROLLER]** may incur arising out of any failure by **[PROCESSOR]** or its employees to comply with any of its obligations under this Contract.

16. Ownership

16.1. All right, title and interest in the Confidential Information shall vest solely with **[CONTROLLER]** or its licensees.

17. Confidentiality

17.1. **[PROCESSOR]** shall procure that all Confidential Information disclosed to it by **[CONTROLLER]** under this Contract or which at any time during the term of the Contract come into **[PROCESSOR]**'s knowledge, possession or control, shall be kept secret and confidential and shall not be used for any purposes other than those required or permitted by this Contract and shall not be disclosed to any third party except insofar as this may be required for the proper operation of this Contract and then only under appropriate confidentiality provisions approved in writing by **[CONTROLLER]** .

17.2. **[PROCESSOR]** will ensure, pursuant to Article. 29 GDPR, that all persons under their authority process the Controller Data exclusively in accordance with this Agreement, as well as the instructions of **[CONTROLLER]**.

17.3. The obligations of confidence contained in this Clause 17 shall not prevent **[PROCESSOR]** from disclosing information to the extent required by law or for any regulatory purposes, provided that prior written notice is given to **[CONTROLLER]** of such disclosure.

17.4. The obligations of confidence contained in this Clause 7 shall not apply to any information which:

17.4.1. is or becomes generally available to the public through no act or default of **[PROCESSOR]** or its directors, employees or agents; or

17.4.2. **[PROCESSOR]** can demonstrate from its written records, prior to its receipt from **[CONTROLLER]** was in its possession and at its free lawful disposal; or

17.4.3. **[PROCESSOR]** can demonstrate from its written records, is after its receipt from **[CONTROLLER]**, generated by employees of **[PROCESSOR]** independently of, and without knowledge of, the Confidential Information; or

17.4.4. **[PROCESSOR]** can demonstrate from its written records, is subsequently disclosed to it without any obligation of confidence by a third party who has not derived it directly or indirectly from **[CONTROLLER**].

17.5. The obligations of confidence contained in this Clause 17 shall survive the termination of this Contract for whatever reason for a period of: (i) three (3) years following the final disclosure of the Confidential Information by **[CONTROLLER]** to **[PROCESSOR];** or (ii) if longer, but only to the extent reasonably required, for as long as the ongoing confidentiality of the Confidential Information, or any part thereof, remains of value to **[CONTROLLER] and** or its interests.

18. Termination

18.1. This Contract may be terminated by **[CONTROLLER]** giving not less than 3 months written notice to **[PROCESSOR]**

18.2. This Contract may be terminated by the **[PROCESSOR]** giving not less than 3 months written notice to **[CONTROLLER]**

19. Consequences of Termination

19.1. On termination of this Contract for whatever reason, **[PROCESSOR]** shall cease to process the Personal Data and Confidential Information and shall arrange for the prompt and safe return of all of the Personal Data and Confidential Information, processed under the terms of this Contract to Controller, together with all copies of the Personal Data in its possession or control or that of its agents or contractors, within such time and by such secure means as **[CONTROLLER]** shall provide for in writing at the time of termination of the Contract.

19.2. On termination of this Contract, should **[CONTROLLER]** require the deletion of Controller Data still held by **[PROCESSOR]** then **[PROCESSOR]** should provide written evidence to support the deletion activity.

19.3. Termination of this Contract shall not affect any rights or obligations of either Party which have accrued prior to the date of termination and all provisions which are expressed to, or do by implication, survive the termination of this Contract shall remain in full force and effect.

20. Notices

20.1. Any notice under or in connection with this Contract shall be in either via email, or in writing sent by courier or by recorded or registered mail to the following addresses:

Notices to **[PROCESSOR]:** Rapid IT Recycling Ltd

Address: Tech Warehouse, Wyre St., Padiham, Lancs., BB12 8DF

Marked for the attention of: Compliance Manager

Notices to **[CONTROLLER]:** _____

Address: _____

Marked for the attention of: _____

A notice shall become effective on the date it is delivered to the address of the recipient Party shown above. A Party may notify the other of a change to its notice details.

20.2. Local Supervisory Authority for the purposes of this contract is agreed to be the UK, Information Commissioners Office.

21. Severability

21.1. Should any provision of this Contract be held to be illegal, invalid or unenforceable in any respect by any judicial or other competent authority under the law of any jurisdiction:

21.2. If by substituting a shorter time period or more restricted application of the provision, it would be valid and enforceable, such shorter time period or more restricted application shall be substituted.

21.3. If Clause 18.1 is not applicable:

21.3.1. such provision shall, so far as it is illegal, invalid or unenforceable in any jurisdiction, be given no effect by the Parties and shall be deemed not to be included in this Contract in that jurisdiction;

21.3.2. the other provisions of this Contract shall be binding on the Parties in that jurisdiction as if such provision were not included herein;

21.3.3. the legality, validity and enforceability of the provision in any other jurisdiction shall not be affected or impaired; and

21.3.4. the Parties shall negotiate in good faith to agree an alternative provision in terms which as closely as possible achieve the intention of the Parties in the original provision, do not substantially impair the Parties' original interests and do not render such provisions invalid or unenforceable.

22. Variation

22.1. No variation or amendment to this Contract shall bind either Party unless made in writing and signed by duly authorised officers of both Parties.

Waiver and Remedies

22.2. A failure to exercise or any delay in exercising any right or remedy provided by this Contract or by law does not constitute a waiver of that right or remedy or a waiver of any other rights or remedies.

23. Entire Contract

23.1. This Contract constitutes the entire Contract and understanding of the Parties relating to its subject matter and supersedes all prior proposals, Contracts and understandings between the Parties or their advisors relating to such subject matter.

23.2. Each of the Parties hereby acknowledges and agrees that in entering into this Contract, it does not rely on any statement, representation, warranty, undertaking, Contract or understanding of any nature whatsoever made by any person other than as expressly included in this Contract as a warranty (a “Prior Representation”) and to the extent that it is so included that Party’s only remedy shall be a contractual one for breach of warranty under the terms of this Contract for damages. To the extent that, notwithstanding the foregoing a Prior Representation has been made and relied upon by either Party, the relevant party unconditionally and irrevocably waives any claims, rights or remedies it may have in relation thereto.

23.3. Nothing in this Clause 4 or in this Contract shall operate to limit or exclude any liability of either Party, or the remedies available to either Party for fraud, including fraudulent acts and/or fraudulent misrepresentations.

24. Further Assurance

24.1. The Parties shall execute all further documents as may be reasonably necessary or desirable to give full effect to the terms of this Contract and to protect the rights of the Parties under it.

26. Governing Law

26.1. This Contract shall be governed in all respects by the laws of England and Wales and each Party hereby irrevocably submits for all purposes in connection with this Contract to the exclusive jurisdiction of the English Courts.

IN WITNESS whereof this Contract consisting of this and the preceding 12 pages and the attached Schedules part is executed as follows:

Signed for and on behalf of the said **[CONTROLLER]**

Signature _____

Print Name _____

Job Title _____

Date _____

This agreement, and the information provided by both the **[CONTROLLER]** and **[PROCESSOR]** will remain valid for a period 24 months from the date of signature unless otherwise superseded by a revised agreement. Should a revised agreement be generated and signed, this invalidates any contracts or agreements held prior.

Schedule 1 Data Subject Rights Request Process

In addition to Clause 10 of this contract, the PROCESSOR agrees to follow the following process when required to do so by the CONTROLLER.

The Rights of Access

The General Data Protection Regulation (GDPR), under Article 15, gives individuals the right to request a copy of any of their personal data which is being 'processed' (i.e. used in any way) by 'controllers' (i.e. those who decide how and why data are processed), as well as other relevant information.

Rapid IT Recycling Ltd will adopt the following procedure in response to any DSAR'S received:

PROCEDURE:

Step 1 – Request

Upon receipt of a DSAR, the Data Protection Officer (DPO) will log and acknowledge the request.

Step 2 – Identify verification

The DPO will check the identify of anyone making a DSAR to ensure information is only given to the person who is entitled to it or who is authorised to act on behalf of the data subject.

If the identity of a DSAR requestor has not already been provided, the DPO will ask the requestor to provide two forms of ID, one of which must be a photo ID and the other confirmation of address.

Step 3 – Information for DSAR

Upon receipt and scrutinisation of the required documents, the DPO will notify the requestor that his/her DSAR will be responded to within 30 calendar days. (The 30-day period begins from the date the required documents are received). The requestor will be informed by the DPO in writing if there will be any deviation from the 30-day timeframe due to other intervening events.

Step 4 – Review of Information

The DPO will collate the relevant and required information as requested in the DSAR.

The DPO shall ensure that the information is reviewed/received by the imposed deadline to ensure the 30-calendar day timeframe is not breached.

The DPO will complete a 'Data Subject Response Form' to document compliance with the 30-day requirement.

Step 6 - Archiving

After the response has been sent to the requestor, the DSAR will be considered closed and archived by the DPO.

Schedule 2 Breach Notification Process

In addition to Clause 12.0 of this contract, the PROCESSOR agrees to adhere to the following process when required to do so by the CONTROLLER.

DATA BREACH PROCEDURE

Introduction

This document sets out the procedure to be followed for suspected or actual personal data breach incidents and must be read in conjunction with Rapid IT's Data Protection Policy.

Purpose and scope

The purpose of this procedure is to provide a framework within which Rapid IT will ensure compliance with its legal obligations in respect of incidents.

This procedure applies to staff, agency workers, contractors and third-party agents who process data for or on behalf of Rapid IT and it must be complied with in the event of a suspected or actual personal data breach.

Rapid IT is required to keep a record of all personal data breaches. Some of these breaches must be reported to the Information Commissioner ("ICO") with undue delay and, at the latest, within 72 hours of detection. It may also need to notify individuals affected by the breach.

It is vital that all staff report a suspected or actual personal data breach, however minor, as soon as possible after discovery so that our Data Protection Officer can investigate promptly and report to the ICO at the latest within 72 hours. Failure to report a personal data breach to the ICO (or to individuals) or a delay in doing so can result in criticism of our company by the ICO and, in serious cases, result in a fine.

Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access, to personal data.

Examples of personal data breaches

- Loss or theft of media or equipment containing personal data (encrypted and non-encrypted devices), e.g. loss of paper record, laptop, iPad or USB stick
- Inappropriate access controls allowing unauthorised use, e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to personal data or information systems
- Equipment failure resulting in personal data being unavailable
- Human error, e.g. email containing personal data sent to the incorrect recipient
- Unauthorised disclosure of sensitive or confidential information, e.g. document posted to an incorrect address or addressee
- Unforeseen circumstances such as a fire or flood resulting in damage or destruction of personal data
- Hacking attack resulting in a breach of confidentiality, effect on the integrity of personal data or its availability
- 'Blagging' offences where personal data is obtained by deceiving the organisation who holds it
- Insecure disposal of paperwork containing personal data

Why should breaches be reported?

The longer an incident goes unreported, the harder it gets to resolve any vulnerabilities. Impacted data subjects have a right to know that their data may have been compromised and that they could take steps that could minimise an adverse impact on them such as informing their bank that their bank details have been compromised.

The longer an incident goes unreported, the longer a vulnerability may remain unaddressed allowing the incident to escalate or for further incidents to occur. Without timely visibility of the incident through Reporting, Rapid IT may not be able to fulfil its legal obligations. The EU General Data Protection Regulations (GDPR) places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office (in the UK's case) without undue delay but within **72 hours of becoming aware of the breach.**

Knowing that a breach has occurred and delaying reporting reduces the time available for the investigation team to understand and assist with a response and still meet privacy compliance requirements.

Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust to prevent future breaches and protect personal data.

Purpose and scope

Procedure for reporting a personal data breach incident

Responsibility for reporting a suspected breach lies with the person who discovered the breach.
Suspected personal data breach incidents should be reported immediately upon discovery, to our Data Protection Officer. You should also inform your line manager unless there is a need to report it confidentially.

Rapid IT will investigate the breach and, where appropriate, notify or involve the relevant line management and HR.

Breach reporting – to the Information Commissioner's Office (ICO)
The DPO (or nominated deputy) upon instruction from Rapid IT will notify the ICO, without undue delay, of a reportable personal data breach.

Breach notification - data subject
Where the personal data breach is likely to result in a high risk of harm to individuals Rapid IT will notify them without undue delay.

Breach notification - to a third party
Where the personal data breach is likely to result in harm to individuals, Rapid IT shall notify any affected third parties (e.g. joint data controller/ to the controller where Rapid IT is the Data Processor) without undue delay. Rapid IT may also need to notify others, e.g. the Police and insurers.

Enforcement
Failure to adhere to this procedure, delay in reporting suspected of actual breach and non-reporting of breaches, may result in disciplinary action in accordance with Rapid IT's Procedure.

Review
This procedure will be reviewed annually or where significant changes have occurred.

Schedule 3 Sub-processors approved by the Controller.

For the purposes of executing this contract, the CONTROLLER approves the use of the SUB-PROCESSORS in the table below. The PROCESSOR confirms there are contracts in place with each SUB-PROCESSOR with terms equivalent to the terms contained within this contract.

Sub Processor Name	Service being Provided	Location where Service delivered	DPO Details at Sub Processor

The above is not applicable to Rapid IT Recycling Limited (Sub-processors are not used by Rapid IT Recycling Limited).

Schedule 4 Data Processing Services

CONTROLLER agreed for the PROCESSOR to perform the following services to achieve the objective of this contract.

LOGISTICAL SERVICES

Agreement for logistical services to include multi-point collections if required during service provision.

CUSTODY & LIABILITY OF CONTROLLER'S DATA

Acknowledgement that the processor accepts custody and liability for the Controller's data at point of collection and issue of either: waste transfer note; hazardous waste transfer note; collection note.

AUDITING DETAIL

Rapid IT Recycling Ltd guarantees clients, or their appointed agent, the access rights, information rights, and inspection rights necessary for the purpose of auditing. Rapid IT Recycling Ltd will guarantee access to the data processing facilities, files, and other documents to allow for monitoring and auditing of the relevant data processing facilities, files and other documentation relating to the processing of the Client's data. Rapid IT Recycling Ltd will provide their clients, or an agent appointed by the same, with all information necessary for the inspection.

SANITISATION PROCESS

Data Destruction/Cleansing

Our data destruction services are undertaken by our in-house fully vetted IT professionals using either overwriting software appropriate to the job or physical destruction which would include crushing or shredding.

Typically, all data bearing assets will be data sanitised using secure overwriting software that has been both 'claims tested' and 'product assured' by ADISA.

Detailed audit reports will be generated detailing the inventory of the assets processed and the means and evidence of end point sanitisation.

Any data bearing asset that fails the erasure process, or is not commercially viable for wiping, will be destroyed on site at Rapid IT using an ADISA 'claims tested' and 'product assured' hard disk crusher or shredder. Likewise, if the original equipment is faulty the drive is removed and physically destroyed.

All loose media is shredded on-site at Rapid IT with a platter and / or NAND cells being physically impaired to stop operation and then mixed for aggregation.

A typical agreement could encompass all forms of IT related WEEE to include, but not limited to:

DATA BEARING ITEMS
Apple Mac Equipment
Back-Up Devices
Combi PC
Copiers / Plotters
Desktop PC
Laptop
Loose Hard Drives
Loose Media – Data Tapes / CD ROMs
Mobile Phones and Tablets
Point of Sale Equipment
Printer / Fax
Servers / Storage Arrays
Switches / Routers
Telephony Equipment
Terminals / Thin Clients

NON DATA BEARING ITEMS
Batteries
CRT Monitors
Televisions
Medical / Testing Equipment
TFT / LCD Monitors
Toners
UPS
Associated peripheral items.

Schedule 5 Sufficient Guarantees regarding the Processing Activities

LICENCES AND PERMITS: (Legal & regulatory requirements to undertake services)	
Waste Carrier Licence Number	CBDU83206
Waste Carrier Licence Number (NI)	ROCUT 8893
T11 Exemption	EXP/TP3741YD
AATF	WEE/GL0002ZS/ATF

ACCREDITATIONS (Evidence & validation of competence to provide services)	
ISO 9001:2015	225152020 (Annual External Audit)
ISO 14001:2015	225162020 (Annual External Audit)
ISO 27001:2013	261762020 (Annual External Audit)
BS 15713	261772020 (Annual External Audit)
ICO	ZA241357 (Annual Subscription)
Cyber Essentials	IASME-CE-032441 (Annual Renewal)
ADISA 8.0 Standard Certification	AAC124

ADISA CERTIFICATION Code of Conduct v.4.0

ADISA Certification Limited champions the business process of asset recovery which is a high-risk process where physical IT assets undergo rigorous processing to ensure the data is sanitised before being tested for resale or recycled for materials recovery. This code of conduct sets out professional standards and principles for both ADISA and Members to follow .

ADISA Code of Conduct Set of Principles:

- Integrity
- Duty to ADISA Certification Scheme
- Monitoring
- Professional Competence
- Duty to fellow members and the profession

Auditing
To become certified an applicant must pass an ADISA full audit. After each full audit, an assessment of the capabilities of the applicant against the criteria which have DIAL options will be made. There are 30 separate assessments which have a DIAL 1, 2 or 3 level of service. An applicant must meet all criterion against a specific DIAL reference to be classified as having that DIAL Licence which would mean that any data controller who has identified themselves as, for example, DIAL 2, should only place business with a service provider holding a level 2 award.

Once an applicant has passed their first audit, they become a certified ADISA member. ADISA then evaluates that member on an on-going basis by conducting Surveillance Audits. These audits take place twice a year and are predominantly unannounced. (There are three types of Surveillance Audit.

1. Data Capability Audit. Auditor assesses the certified member's data capability statement and the sanitisation tools which they operate. The auditor selects a range of products / media which have been processed and forensically analyses them on site to assess if data can be recovered. Checks are also made on degausser outputs, and screen aperture within shredders if applicable.

2. Process Audit. Here the auditor will assess the process control and will check contamination and segregation throughout. In addition, a sample of at least ten devices will be picked and the paperwork associated with those devices will be requested once the auditor leaves site.

3. Security Audit. The auditor will initially try to gain entry to the facility either in a physical sense or by engineering an opportunity to gain access. Once identified the auditor will then assess the site's security features including CCTV and other physical barriers.

Schedule 6

DATA RETENTION & DISPOSAL POLICY

1. Introduction

While carrying out various functions, Rapid IT Recycling creates and holds a wide range of recorded information. Records will be properly retained to enable Rapid IT Recycling to meet its business needs, legal requirements, to evidence events or agreements in the event of allegations or disputes and to ensure that any records of historic value are preserved.

The untimely destruction of records could affect:

- the conduct of Rapid IT's business.
- the ability of Rapid to defend or instigate legal actions.
- Rapid IT's ability to comply with statutory obligations.
- Rapid IT's reputation.

Conversely, the permanent retention of records is undesirable and disposal is necessary to free up storage space, reduce administrative burden and to ensure that Rapid IT Recycling does not unlawfully retain records for longer than necessary (particularly those containing personal data).

This policy supports Rapid IT Recycling in demonstrating accountability through the proper retention of records and by demonstrating that disposal decisions are taken with proper authority and in accordance with due process.

2. Purpose

The purpose of this policy is to provide guidance regarding the length of time that Rapid IT's records should be retained and the processes to review the records, as to any further retention or for disposing of records at the end of the retention period. The policy helps to ensure that Rapid IT Recycling operates in compliance with the General Data Protection Regulation and any other legislative or regulatory retention obligations.

3. Scope

The policy covers the records listed in the Information Asset Register irrespective of the media on which they are created or held including:

- Paper
- Electronic files (including database, Word documents, power point presentations, spreadsheets, webpages and e-mails).
- Photographs, scanned images, CD-ROMs and video tapes.

And includes all types of records which Rapid IT Recycling creates or holds on behalf of clients. The records may include, but are not limited to, the following:

- Client files
- Contracts and invoices
- Registers
- Financial accounts
- Employee information
- Member information

4. Application

The policy applies equally to full time and part time employees on a substantive or fixed term contract and to associated persons who work for Rapid IT Recycling.

5. Minimum Retention Period

Unless a record has been marked for 'permanent preservation' it will only be retained for a limited period. The retention period of six years applies to all records associated with the client. Records relating to staff of Rapid IT Recycling will be retained throughout employment and up to two years after.

The recommended minimum retention period derives from either:

- Business need
- Legislation
- Responses to complaints
- Taking or defending legal action.

6. Disposal

6.1 What is Disposal

The Data Protection Manager is responsible for ensuring that the Information Asset Register is periodically reviewed (annually) to determine whether any retention periods have expired. Once the retention period has expired, the record must be reviewed and a 'disposal action' agreed upon.

A 'disposal action' is;

- The destruction of the record; or
- The retention of the record for a further period under the instruction from the Data Controller of the data; or,
- Alternative disposal of the record

6.2 Making and Recording the Disposal Decision

A review of the record will take place as soon as possible after the expiry of the retention period or, if that is not feasible, the record will be retained and a later review date set.

The disposal decision will be reached having regard to:

- On-going business and accountability needs (including audit)
- Current applicable legislation
- Whether the record has any long-term historical or research value;
- Best practice
- The legal, political and reputational risks associated with keeping, destroying or losing control over the record.

Decisions will not be made with the intent of denying access or destroying evidence.

7. Destruction

No destruction of a record will take place without assurance that:

- The record is no longer required by any member of Rapid IT Recycling;
- No litigation or investigation is current or pending which affects the record
- There are no current or pending GDPR subject access requests which affect the record.

8. Destruction of Paper Records

Destruction will be carried out in a way that preserves the confidentiality of the record. Non-confidential records will be placed in ordinary rubbish bins or recycling bins. Confidential records will be shredded. A certificate of destruction will be retained upon each completed process. All copies including security copies, preservation copies and backup copies will also be destroyed at the same time in the same manner.

9. Destruction of Electronic Records

All electronic records will be either physically destroyed or data wiped. Confirmation of the date of this will be recorded alongside records of all other types of data deletion.

10. Further Retention

The record may be retained for a further period if it has on-going business value or if there is specific legislation which requires it to be held for a further period.

11. Further Information

This policy should be read in conjunction with the Rapid IT's Data Protection Policy.

Schedule 7 Rapid IT Recycling Limited Credentials

Rapid IT will maintain the following during the contract:

LICENCES AND PERMITS:	
Waste Carrier Licence Number	CBDU83206
T11 Exemption	EXP/TP3741YD
AATF	WEE/GL0002ZS/ATF

ACCREDITATIONS:	
ISO 9001:2015	225152020
ISO 14001:2015	225162020
ISO 27001:2013	261762020
BS 15713	261772020
ICO	ZA241357
Cyber Essentials	IASME-CE-032441
ADISA 8.0 Standard Certification	AAC124

INSURANCES:	
Employee Liability	£10,000,000
Public Liability	£2,000,000
Professional Indemnity	£1,000,000
Cyber Insurance	£2,000,000
Products Liability	£2,000,000