H TEMPEST LIMITED

GENERAL DATA PROTECTION POLICY

GENERAL DATA PROTECTION POLICY

SECTION

H TEMPEST LIITED

GENERAL DATA PROTECTION POLICY

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 We have adopted this General Data Protection Policy as part of our overall suite of data protection and information security policies. That suite also includes:

- Acceptable Usage Policy
- Bring Your Own Device (BYOD) Policy
- Data Retention and Destruction Policy
- Information Security Policy
- Policy on Complying with Individuals' Data Protection Rights
- Policy on Using Personal Data in Marketing
- Privacy Notice
- Third Party Supplier Policy
- And such other policies relating to data protection, privacy, information and data security as we may adopt from time to time.

1.3 The above policies, including this one, are known collectively as our Data Protection and Information Security Policies, or simply "**the Policies**".

1.4 Data users within our organisation (whether officers, employees, contractors, consultants, agents, interns, volunteers, casual workers, agency workers or otherwise), and anyone else who has access to our IT and communications systems, are obliged to comply with the Policies when processing personal data on our behalf or using our information systems. Any breach of the Policies may result in disciplinary action up to and including dismissal and in some circumstances may constitute a criminal offence.

1.5 The Policies do not form part of any employee's contract of employment and may be amended at any time. However, all employees, contractors and other workers are required to be made aware of the Policies and to follow it. Failure by anyone to follow any of the Policies may amount to misconduct or gross misconduct depending on the severity of the failure.

2. ABOUT THE POLICIES

2.1 This Policy sets the scene for many of the other Policies. It sets out some principles of general application to our processing of personal data which we must comply with. It also provides high level statements on a number of matters that are dealt with in more detail in the other individual Policies. Data users should read this Policy first to familiarise themselves with the general data protection issues, and then familiarise themselves with the more specific requirements of the other Policies.

2.2 The types of personal data that H Tempest (we) may be required to handle include information about current, past and prospective suppliers, customers, employees, contractors and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in data protection law.

2.3 Data protection law in the UK is, with effect from 25 May 2018, embodied largely in the European General Data Protection Regulation (**GDPR**). References in the Policies to "**Data Protection Law**" are references to the GDPR and any laws subordinate to it, as the same may be amended or replaced from time to time.

2.4 The Policies, and any other documents referred to in them, set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources, and the rules and legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Data Protection Manager (or DPM) is responsible for ensuring our compliance with Data Protection Law and with the Policies. That post is held by Mark Johns, Head of IT ansd Data, Tel: 01736751488, email: m.johns@htempest.co.uk. Any questions about the operation of the Policies or any concerns that any of the Policies have not been followed should be referred in the first instance to the DPM. See section 21 for further details.

3. DEFINITIONS OF DATA PROTECTION TERMS

The following terms are used in the Policies.

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of the Policies include all living individuals about whom we hold personal data. A data subject need not be a UK or EU national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means any data relating to a living identified or identifiable individual, including any individual who can be identified directly or indirectly by reference to an identifier such as a name, identification number, location, date, online identifier or some other factor specific to that individual. Personal data can be factual (for example, a name, address, email address date of birth or financial information) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Law. We are the data controller of all personal data used in our business for our own commercial purposes, as set out in our Record of Processing (see below).

3.5 **Data users** are those of our workers (whether employees, contractors or other representatives) whose work involves processing personal data or other information. Data users must protect the data they handle in accordance with the Policies and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf. We may also act as a data processor to the extent that we process personal data on behalf of our clients who are data controllers, as set out in our Record of Processing (see below).

3.7 **ICO** means the UK's Information Commissioner's Office.

3.8 **legitimate interests** means legitimate interests pursued by us as a data controller or a third party, unless those interests are overridden by the interests or fundamental rights or freedoms of the data subject which require the protection pf personal data. Our legitimate interests will include the conduct of our business and marketing our business unless overridden by any of the factors mentioned above.

3.9 **Privacy Notice** means the privacy notice that we adopt from time to time setting out the principles of privacy that we will communicate to individuals about whom we process data.

3.10 **Processing** is any activity that involves any kind of operation on personal data. It includes obtaining, recording, holding organising, structuring, storing, adapting, altering, amending, retrieving, consulting, using, disclosing, erasing or destroying it. Processing also includes transferring personal data or otherwise making it available to third parties, as well as alignment, combination and restriction.

3.11 **Record of Processing** means the record of data processing that we are required to keep by Data Protection Law, setting out the purposes for which we process personal data, the categories of data subjects, the categories of personal data and other such matters.

3.12 **Special categories of personal data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sexual life or sexual orientation. For the purposes of the Policies, it also includes information about the commission of, or proceedings relating to any offence committed or alleged to have been committed by a person, the disposal of such proceedings or the sentence of any court in such proceedings. Special categories of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned. Any processing of special categories of personal data should be described in our Record of Processing.

3.13 **Central Data Processing Files** means the central files relating to our data processing activities, in which are stored all of the Policies together with our Record of Processing, all outcomes of appraisals and Data Protection Impact Assessments carried out under the Technology Appraisal Policy, all reports compiled under the Third Party Supplier Policy, records of all responses to data subjects following their exercise of data protection rights, all communications with the Information Commissioner's Office, and all other decisions or other documents relevant to our data protection compliance.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the enforceable principles of Data Protection Law. These provide that personal data must be:

(a) Processed fairly, lawfully and transparently;

(b) Processed for specified, explicit and legitimate purposes and not in any further way;

(c) Adequate, relevant and limited to what is necessary for the purpose;

(d) Accurate and, where relevant, kept up to date;

(e) Not kept in a form which permits the identification of individuals for any longer than necessary for the purpose;

(f) Kept in a secure manner;

Personal data must also be processed in accordance with individuals' rights, and not transferred to people or organisations situated in countries without adequate protection. See further below.

5. FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1 Data Protection Law is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, it must be processed on the basis of at least one of the legal grounds set out in Data Protection Law. These include, among other things, the data subject's consent to the processing, that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interests of the data controller or the party to whom the data is disclosed. When special categories of personal data are being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process the personal data set out in our Record of Processing. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others), as set out in further detail in the Record of Processing.

6.2 We will process personal data for the specific purposes set out in this Data Protection Policy or the Record of Processing or for any other purposes specifically permitted by Data Protection Law. We will notify the applicable purposes to the data subject when we first collect the data or, where the data comes from a third party, as soon as possible thereafter, as set out at section 7 below.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) Our identity and contact details;

(b) The purpose or purposes for which we intend to process that personal data;

(c) The basis on which we are processing the personal data, as referred to at section 5.2 above;

(d) The period for which we will hold the personal data, or if that is not possible, the criterial used to determine that period;

(e) The types of third parties, if any, with which we will share or to which we will disclose that personal data;

(f) The existence of various rights of individuals, and methods by which those rights can be exercised.

7.2 We will achieve this notification by having those details set out in our Privacy Notice, and taking reasonable steps to make sure that everyone who submits personal data to us has their attention drawn to the Privacy Notice, which will be made available to them as applicable.

7.3 If we receive personal data about a data subject from other sources, we will provide or make available to the data subject the information specified in section 7.1 as soon as possible thereafter.

8. DISCLOSING PERSONAL DATA

8.1 It is a fundamental principle of Data Protection Law that we must not disclose any personal data relating to any data subject to another person unless one of a very limited number of exceptions apply. Accordingly, if any Data user is asked to disclose personal data about one or more individuals to a person other than the data subject themselves, the response should generally be that such a disclosure is not permitted due to Data Protection Law.

8.2 Note that 8.1 applies even where we are providing information to a data subject him/herself – if that information includes data about another individual, we must consider carefully whether we can disclose it, make any edits or redactions to the information prior to disclosure, or refuse to disclose it on the grounds that disclosure would have to involve the disclosure of information about another individual.

8.3 If we decide that information should not be disclosed for the reasons set out above, and the person requesting that information wishes to take the matter further, they should be referred to our DPM. Staff should not be bullied into

disclosing personal information. It is safer not to disclose the information rather than disclose it if you are unsure – in those circumstances you must consult the DPM. Wrongly disclosing information may be a serious breach of Data Protection Law requiring reporting to the ICO and/or the affected data subjects.

8.4 See also section 9 below and our Policy on Complying with Individuals' Data Protection Rights in relation to requests for personal data.

8.5 Our Privacy Notice sets out the extent to which we may disclose data to third parties – the commitments set out in that document must be followed at all times.

8.6 Where we are to disclose personal data to a third party, we must consider whether a data sharing or other form of agreement is required in order to enable us to comply with Data Protection Law in relation to such disclosure. Accordingly, the DPM must be consulted before any arrangement is put in place to disclose personal data to a third party.

9. COMPLYING WITH INDIVIDUALS' RIGHTS

9.1 Data Protection Law gives individuals various rights in relation to information that we may hold about them. These include the right to access data that we hold about them (known as the subject access right), the right to require us not to use their personal data for direct marketing purposes, the right to ask us to rectify incorrect data, and the right to be forgotten. Some of these rights only apply in limited circumstances.

9.2 Those rights include:

(a) The right to ask us not to process their personal data for direct marketing purposes, even if they have given consent;

(b) If our processing is based on their consent, the right to withdraw any consent they may have given for our processing of their data – if they exercise this right, we will be required to stop such processing if consent is the sole lawful ground on which we are processing that data;

(c) The right to ask us for access to the data we hold about them;

(d) The right to ask us to rectify any data that we hold about them that is inaccurate or incomplete;

(e) The right to ask us to delete their data in certain circumstances;

(f) The right to ask us to restrict our processing of their data in certain circumstances;

(g) The right to object to our processing of their data in certain circumstances;

(h) In certain circumstances, the right to require us to give them the data we hold about them in a structured, commonly used and machine-readable format so that they can provide the data to another data controller;

(i) The right not to be subject to decisions made on an automated basis.

9.3 If we receive a request from an individual in respect of any of the above, we must follow the procedure set out in our Policy on Complying with Individuals' Data Protection Rights.

9.4 We may from time to time be contacted by individuals with enquiries relating to their relationship with us, for example account information. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if we have checked the caller's identity to make sure that information is only given to a person who is entitled to it. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked. That written request can then be treated as a subject access request under our Policy on Complying with Individuals' Data Protection Rights.

10. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

10.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

10.2 We may update and use derived or inferred data using algorithms and other appropriate mathematical or statistical gathering programmes that analyse various forms of data provided that such data has been anonymised and does not constitute personal data.

11. ACCURATE DATA

11.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11.2 Staff should take every opportunity to ensure that data is kept accurate and up to date, for instance confirming a customer's details when they call. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number or email address, it should be removed from the database.

11.3 It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files.

12. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. Further detail on this is set out in our Data Retention and Destruction Policy.

13. USING PERSONAL DATA FOR MARKETING

If we wish to use any personal data for marketing purposes, we must ensure that such use complies with our Policy on Using Personal Data in Marketing, and with the relevant aspects of our Privacy Notice.

14. DATA SECURITY

14.1 We will process all personal data we hold in accordance with our Information Security Policy.

14.2 We endeavour to develop the security, technical integrity and structure of our system organisation and to preserve our system capabilities.

15. DATA PROTECTION AND STAFF

15.1 Members of staff should be trained and supervised in respect of the handling and management of personal information; including inductions for new staff members.

15.2 Persons engaged by us are duty bound by obligations of confidentiality with regard to confidential information in their employment or consultancy contracts.

16. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

16.1 We may NOT transfer any personal data we hold to a country outside the European Economic Area ("EEA") unless one of the following conditions applies to that transfer:

(a) The country to which the personal data are transferred has been certified by the European Commission as providing an adequate level of protection for the data subjects' rights and freedoms.

(b) The transfer is subject to one of the safeguards set out in Article 46 of the GDPR, which include where the transfer is carried out under the auspices of the EU-US Privacy Shield or on the basis of contractual terms approved by the European Commission; or

(c) The transfer is made in one of the circumstances listed in Article 48 of the GDPR, which include:

- where the individual has explicitly consented to the transfer, after having been informed of the related risks of the transfer;
- where the transfer is necessary for the performance of a contract between the individual and the data controller, or the implementation of pre-contractual measures taken at the individual's request; or
- where the transfer is necessary for the conclusion or performance of a contract entered in the interest of the individual by the data controller and some other person (e.g. the delivery of a product as a gift).

16.2 If we are asked to transfer any personal data outside the EEA, or if we are considering a relationship with a third party such as a supplier or customer pursuant to which personal data would be transferred outside the European Economic Area, we must consult the DPM first to ensure that one of the conditions is met.

16.3 Any transfers of personal data outside the EEA should be summarised in our Record of Processing.

17. SELECTING DATA PROCESSORS

17.1 If we are to appoint any other person to carry out any service for us which will involve them having access to personal data that we hold, it is likely that they will be our data processor or (if we are acting as a data processor in respect of that data) our data sub-processor. In such event, we must follow the procedure set out in the Third Party Supplier Policy. Details of our data processors must be recorded in our Record of Processing.

18. DATA BREACHES

18.1 It is an essential obligation under Data Protection Law to report personal data breaches as follows:

(a) Unless the breach is unlikely to result in any risk to the rights or freedoms of individuals (see below), we must report the breach to the ICO as soon as possible and, where feasible, within 72 hours of the breach;

(b) Where the breach is likely to result in a high risk to the rights or freedoms of any individual, we must notify the affected individuals as soon as possible.

18.2 A data breach may need not just be a deliberate external act such as hacking. It includes losing any device on which personal data may be stored or accessible. It includes where a member of staff carries out an act in relation to

data that he or she is not authorised to carry out. It can also include accidental loss, destruction or corruption of data.

18.3 A risk to the rights or freedoms of individuals will arise, for example, if the breach is likely to result in detriment to the individual such as discrimination, damage to reputation, financial loss, loss of confidentiality, or other social or economic disadvantage. This needs to be assessed on a case by case basis. Accordingly, if any staff member becomes aware of a data breach, it must be reported immediately to the DPM so that a swift assessment can be made of the next steps to be taken.

19. RECORD OF PROCESSING AND CENTRAL DATA PROCESSING FILES

19.1 We are required to keep a Record of Processing, setting out:

(a) The name and contact details of the data controller;

(b) The name and contact details of any data controller with whom we are joint data controllers in respect of any personal data;

(c) The name and contact details for each such data controller;

(d) The purposes for which we are processing data;

(e) A description of the categories of data subjects about whom we may process data;

(f) A description of personal categories of personal data that we may process.

(g) The categories of recipient (if any) to whom personal data may be disclosed;

(h) Any transfers of personal data to countries outside the UK;

(i) Where possible, the envisaged data retention time limits for data, beyond which the data will be deleted;

(j) A general description of the technical and organisational measures that we have in place to ensure a level of security in relation to the personal data that we hold and otherwise process.

19.2 The Record of Processing will be kept in our Central Data Processing Files. The Central Data Processing Files are the responsibility of the DPM, and access to such files will be subject to the control of the DPM.

20. DATA PROTECTION APPRAISALS

In considering whether to implement any new technology or processes that will include personal data, we must consider the following:

20.1 We are required by the GDPR to follow an approach of "data protection by design and by default" approach in respect of any such implementation. In doing so, we must, amongst other things, document an appraisal of the implementation ("Implementation Appraisal"), as described and required by our Data Protection Appraisal Policy. We will keep each completed Implementation Appraisal with our Central Data Protection Records.

20.2 We will conduct Data Impact Assessments (**DPIAs**) where required to do so as a result of the application of our Data Protection Appraisal Policy.

20.3 We will make available our DPIAs to the ICO on request.

20.4 We are obliged to consult with the ICO where residual risk is high and in the event that such risks cannot be sufficiently identified by us. In this event, the DPM should be involved at an early stage to lead the consultation with the ICO.

21. DATA PROTECTION MANAGER

21.1 We have taken the policy decision that the appointment of a DPM is desirable in order to assist us in achieving compliance with Data Protection law.

21.2 DPM is responsible for informing and advising employees in respect of compliance with data protection legislation and monitoring compliance in relation thereto, and serves as a first point of contact for the ICO and for data subjects.

21.3 Our DPM is also responsible for the maintenance of our data protection records, the internal management of data protection activities, staff training, internal audit and reporting to senior management at Board level.

22. REVIEW, REPORTING AND CHANGES TO THE POLICIES

22.1 The Policies must be kept under review as required, and in any event will be reviewed not less than annually. Responsibility for such review lies with the DPM.

22.2 The DPM should keep developments in Data Protection Law, and related areas such as information security, as well as particular risks faced by our business, under review, and initiate such steps as may be considered necessary in order to ensure that the Policies best meet the requirements of Data Protection Law.

22.3 Not less than once per year, the DPM will submit a written report to the Board setting out all matters arising during the preceding year relating to data protection. The DPM will be invited to present that report in person to the Board, and the Board will take full account of the report.

22.4 We reserve the right to change the Policies at any time. Where appropriate, we will notify those affected of the changes by appropriate methods.