Personal Data Protection Policy
Incorporating the General Data Protection Regulation (GDPR)

1. Introduction

This Policy sets out the obligations of Owen Fabrication Ltd, a company registered in England under number 04142278, whose registered office is at Yard1, Canal Wharf, Horsenden Lane North, Greenford Middlesex,UB6 7PH regarding data protection and the rights of its employees (in this context, "employee data subjects") in respect of their personal data under Data Protection Law (all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, EU Regulation 2016/679 General Data Protection Regulation ("GDPR"), the Data Protection Act 2018, and any successor legislation or other directly applicable EU regulation relating to data protection and privacy for as long as, and to the extent that, EU law has legal effect in the UK).

This Policy sets out the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, and other parties working on behalf of the Company.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to employee data subjects;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom the Company holds personal data (in this context, employee

	data subjects);
“EEA”	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
“personal data”	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
“personal data breach”	means 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;
“processing”	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“pseudonymisation”	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
“special category personal data”	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. **Scope**

3.1 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it works.

3.2 The Company's data Protection Officer is James Doherty, email: james@owenfab.co.uk. The Data Protection Officer is responsible for working together with the Managers and departments, for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

3.3 All Managers, department heads and supervisors are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.4 Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which employee personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and process employee personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of employee personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of an employee data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect employee personal data;

h) if employee personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if employee personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when employee personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out;

m) if any assistance is required in complying with the law applicable to direct marketing.

4. The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The GDPR sets out the following principles with which anyone handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject;

4.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

The GDPR sets out the following key rights applicable to data subjects:

5.1 the right to be informed;

5.2 the right of access;

5.3 the right to rectification;

5.4 the right to erasure (also known as the 'right to be forgotten');

5.5 the right to restrict processing;

5.6 the right to data portability;

5.7 the right to object; and

5.8 rights with respect to automated decision-making and profiling.

6. Lawful, Fair, and Transparent Data Processing

6.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful only if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6.2 If the personal data in question is special category personal data (also known as 'sensitive personal data'), at least one of the following conditions must be met in addition to one of the conditions set out above:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social

protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

e) the processing relates to personal data which is manifestly made public by the data subject;

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

g) the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and

provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing any personal data, the following shall apply:

7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

7.5 Where special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

8.1 The Company collects and processes the employee personal data set out in Parts 23 to 28 of this Policy. This includes:

a) personal data collected directly from employee data subjects e.g. home address, date of birth, passport number, etc. OR National insurance numbers.

b) Company addresses, bank account numbers, email and phone numbers.

8.2 The Company only collects, processes, and holds employee personal data for the specific purposes set out in Parts 23 to 28 of this Policy (or for other

purposes expressly permitted by Data Protection Law).

8.3 Employee data subjects shall be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

9. Adequate, Relevant, and Limited Data Processing

9.1 The Company will only collect and process employee personal data for and to the extent necessary for the specific purpose or purposes of which employee data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Parts 23 to 28, below.

9.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect employee personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of the Company may process employee personal data only when the performance of their job duties requires it. Employee personal data held by the Company cannot be processed for any unrelated reasons.

10. Accuracy of Data and Keeping Data Up-to-Date

10.1 The Company shall ensure that all employee personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of an employee data subject, as set out in Part 17, below.

10.2 The accuracy of employee personal data shall be checked when it is collected and at **[**regular**]** **OR [a**nnual**]** intervals thereafter. If any employee personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

10.3 It is the responsibility of individual employee data subjects to ensure that the personal data they have provided to the Company is kept up-to-date. If any such personal data changes, employees should ensure that the relevant member of staff and/or department is informed as soon as is reasonably possible. The Company relies on the cooperation of its employees to help meet its obligations under Data Protection Law.

11. Data Retention

11.1 The Company shall not keep employee personal data for any longer than is necessary in light of the purpose or purposes for which it was originally collected, held, and processed.

11.2 When employee personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it securely and without delay.

11.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

12. Secure Processing

12.1 The Company shall ensure that all employee personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 29 to 34 of this Policy.

12.2 All technical and organisational measures taken to protect employee personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of employee personal data.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all employee personal data as follows:

a) only those with a genuine need to access and use employee personal data and who are authorised to do so may access and use it;

b) employee personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access employee personal data as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1 The Data Protection Officer shall be responsible for working together with the HR Department and Managers for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 The Company shall follow a 'privacy by design' approach at all times when collecting, holding, and processing employee personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of employee data subjects (please refer to Part 14 for further information).

13.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

13.4 The Company's data protection compliance shall be regularly reviewed and

evaluated by means of Data Protection Audits.

13.5 The Company shall keep written internal records of all employee personal data collection, holding, and processing, which shall incorporate the following information:

a) the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which the Company collects, holds, and processes employee personal data;

c) the Company's legal basis or bases (including, where applicable, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing employee personal data;

d) details of the categories of employee personal data collected, held, and processed by the Company, and the categories of employee data subject to which that personal data relates;

e) details of any transfers of employee personal data to non-EEA countries including all mechanisms and security safeguards;

f) details of how long employee personal data will be retained by the Company (please refer to the Company's Data Retention Policy);

g) details of employee personal data storage, including location(s);

h) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of employee personal data.

14. Data Protection Impact Assessments and Privacy by Design

14.1 In accordance with the 'privacy by design' principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of employee personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of employee data subjects.

14.2 The principles of 'privacy by design' should be followed at all times when collecting, holding, and processing employee personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

d) the risks posed to employee data subjects and to the Company, including their likelihood and severity.

14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of employee personal data that will be collected, held, and processed;

b) the purpose(s) for which employee personal data is to be used;

c) the Company's objectives;

d) how employee personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) risks posed to employee data subjects;

h) risks posed both within and to the Company; and

i) proposed measures to minimise and handle identified risks.

15. Keeping Data Subjects Informed

15.1 The Company shall provide the information set out in Part 15.2 to every data employee data subject:

a) Where employee personal data is collected directly from employee data subjects, those employee data subjects will be informed of its purpose at the time of collection; and

b) where employee personal data is obtained from a third party, the relevant employee data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the employee data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

15.2 The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, all relevant contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the employee personal data is being collected and will be processed (as detailed in Parts 23 to 28 of this Policy) and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the employee personal data;

d) where the employee personal data is not obtained directly from the employee data subject, the categories of personal data collected and processed;

e) where the employee personal data is to be transferred to one or more third parties, details of those parties;

f) where the employee personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place (see Part 32 of this Policy for further details);

g) details of applicable data retention periods;

h) details of the employee data subject's rights under the GDPR;

i) details of the employee data subject's right to withdraw their consent to the Company's processing of their personal data at any time (where applicable);

j) details of the employee data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the GDPR);

k) where the employee personal data is not obtained directly from the employee data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the employee personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the employee personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

16.1 Employee data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

16.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at james@owenfab.co.uk.

16.3 Responses to SARs must normally be made within one month of receipt; however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the

data subject shall be informed.

16.4 All SARs received shall be handled by the Company's Data Protection Officer **[**in accordance with the Company's Data Subject Access Request Policy and Procedure**]**.

16.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of Personal Data

17.1 Employee data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

17.2 The Company shall rectify the employee personal data in question, and inform the employee data subject of that rectification, within one month of the employee data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.

17.3 In the event that any affected employee personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure of Personal Data

18.1 Employee data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that employee personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the employee data subject wishes to withdraw their consent (where applicable) to the Company holding and processing their personal data;

c) the employee data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

d) the employee personal data has been processed unlawfully;

e) the employee personal data needs to be erased in order for the Company to comply with a particular legal obligation

18.2 Unless the Company has reasonable grounds to refuse to erase employee personal data, all requests for erasure shall be complied with, and the

employee data subject informed of the erasure, within one month of receipt of the employee data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.

18.3 In the event that any employee personal data that is to be erased in response to an employee data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. **Restriction of Personal Data Processing**

19.1 Employee data subjects may, in certain limited circumstances, request that the Company ceases processing the personal data it holds about them. If an employee data subject makes a valid request, the Company shall retain only the amount of employee personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

19.2 In the event that any affected employee personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. **Data Portability**

20.1 The Company processes personal data relating to employees using automated means.

20.2 Where employee data subjects have given their consent to the Company to processing their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the employee data subject, employee data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

20.3 Where technically feasible, if requested by an employee data subject, personal data shall be sent directly to the required data controller.

20.4 All requests for copies of employee personal data shall be complied with within one month of the employee data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the employee data subject shall be informed.**]**

21. **Objections to Personal Data Processing**

21.1 Employee data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing

(including profiling), and processing for scientific and/or historical research and statistics purposes.

21.2 Where an employee data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the employee data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

21.3 Where an employee data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

21.4 Where an employee data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the employee data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

21.5 Health records (Please refer to Part 25, below, for further information):

a) Details of sick leave;

b) Medical conditions;

c) Disabilities;

d) Prescribed medication;

21.6 Employment records:

a) Interview notes;

b) CVs, application forms, covering letters, and similar documents;

c) Assessments, performance reviews, and similar documents;

d) Details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses;

e) Details of trade union membership (please refer to Part 27, below, for further information)

f) Employee monitoring information (please refer to Part 28, below, for further information);

g) Records of disciplinary matters including reports and warnings, both formal and informal;

h) Details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes;

22. **Equal Opportunities Monitoring Information**

22.1 The Company collects, holds, and processes certain information for the purposes of monitoring equal opportunities. Some of the personal data collected for this purpose, such as details of ethnic origin and religious beliefs, falls within the GDPR's definition of special category data (see Part 2 of this Policy for a definition). Where possible, such data will be anonymised. Where special category personal data remains, it will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data, as set out in Part 6.2 of this Policy. **[**No special category personal data relating to equal opportunities monitoring will be collected, held, or processed without the relevant employee data subject's consent.**]** **[**Non-anonymised equal opportunities monitoring information**]** **OR** **[**Equal opportunities monitoring information**]** shall be accessible and used only by HR department and Managers and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company **[**without the express consent of the employee data subject(s) to whom such data relates**]**, except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 6.2 of this Policy.

22.2 Equal opportunities monitoring information will only be collected, held, and processed to the extent required to prevent, reduce, and stop unlawful discrimination in line with the Equality Act 2010, and to ensure that recruitment, promotion, training, development, assessment, benefits, pay, terms and conditions of employment, redundancy, and dismissals are determined on the basis of capability, qualifications, experience, skills, and productivity.

22.3 Employee data subjects have the right to request that the Company does not keep equal opportunities monitoring information about them. All requests must be made in writing and addressed to James Doherty, policy officer, at james@owenfab.co.uk.

23. **Health Records**

23.1 The Company holds health records on **[**all**]** employee data subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In particular, the Company places a high priority on maintaining health and safety in the workplace, on promoting equal opportunities, and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health data on employees falls within the GDPR's definition of special category data (see Part 2 of this Policy for a definition). Any and all data relating to employee data subjects' health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data, as set out in Part 6.2 of this Policy. **[**No special

category personal data will be collected, held, or processed without the relevant employee data subject's express consent.**]**

23.2 Health records shall be accessible and used only by HR Department and Managers and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company **[**without the express consent of the employee data subject(s) to whom such data relates**]**, except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 6.2 of this Policy.

23.3 Health records will only be collected, held, and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

23.4 Employee data subjects have the right to request that the Company does not keep health records about them. All such requests must be made in writing and addressed to James Doherty, policy officer, email; james@owenfab.co.uk.

24. **Benefits**

24.1 In cases where employee data subjects are enrolled in benefit schemes which are provided by the Company, it may be necessary from time to time for third party organisations to collect personal data from relevant employee data subjects.

24.2 Prior to the collection of such data, employee data subjects will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed, as per the information requirements set out in Part 15 of this Policy.

25. **Trade Unions**

25.1 The Company will provide the following personal data concerning relevant employee data subjects to bona fide trade unions where those unions are recognised by the Company. In most cases, information about an individual's trade union membership falls within the GDPR's definition of special category data (see Part 4 of this Policy for a definition). Any and all data relating to employee data subjects' trade union membership, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data, as set out in Part 6.2 of this Policy. **[**No special category personal data will be collected, held, or processed without the relevant employee data subject's express consent. The following data will be collected and supplied:

25.1.1 Name;

25.1.2 Job description;

25.2 All employee data subjects have the right to request that the Company does not supply their personal data to trade unions and shall be informed of that

right before any such transfer is made.**]**

26. **Employee Monitoring**

26.1 The Company may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

26.2 Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

26.3 Monitoring will only take place if the Company considers that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Company's obligations under the GDPR.

26.4 The Company shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using Company equipment or other facilities including, but not limited to, Company email, the Company intranet, or a virtual private network ("VPN") service provided by the Company for employee use.

27. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving employee personal data:

27.1 All emails containing employee personal data must be encrypted.

27.2 All emails containing employee personal data must be marked "confidential";

27.3 Employee personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

27.4 Employee personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

27.5 Employee personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

27.6 Where employee personal data is to be sent by facsimile transmission the

recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

27.7 Where employee personal data is to be transferred in hardcopy form it should be passed directly to the recipient.

27.8 All employee personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”;

28. **Data Security - Storage**

The Company shall ensure that the following measures are taken with respect to the storage of employee personal data:

28.1 All electronic copies of employee personal data should be stored securely using passwords and data encryption;

28.2 All hardcopies of employee personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

28.3 All employee personal data stored electronically should be backed up with backups stored **[**onsite**] AND/OR [**offsite**]**. All backups should be encrypted.

28.4 No employee personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise **[**without the formal written approval of James Doherty, policy officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary**]**;

28.5 No employee personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and employee personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of Data Protection Law, including but not limited to the GDPR, (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

29. **Data Security - Disposal**

When any employee personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

30. **Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of employee personal data:

30.1 No employee personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any employee personal data that they do not already have access to, such access should be formally requested from James Doherty policy office.

30.2 No employee personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of James Doherty policy officer.

30.3 Employee personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

30.4 If employee personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

30.5 **[**Where employee personal data held by the Company is used for marketing purposes, it shall be the responsibility of the policy officer to ensure that the appropriate consent is obtained and that no employee data subjects have opted out, whether directly or via a third-party service such as the TPS.

31. **Data Security - IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

31.1 All passwords used to protect employee personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. **[**All software used by the Company is designed to require such passwords.**]**;

31.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

31.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates.

31.4 No software may be installed on any Company-owned computer or device without the prior approval of the policy officer.

32. **Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of employee personal data:

32.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

32.2 Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, employee personal data in order to carry out their assigned duties correctly shall have access to employee personal data held by the Company;

32.3 All sharing of employee personal data shall comply with the information provided to the relevant employee data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

32.4 All employees, agents, contractors, or other parties working on behalf of the Company handling employee personal data will be appropriately trained to do so;

32.5 All employees, agents, contractors, or other parties working on behalf of the Company handling employee personal data will be appropriately supervised;

32.6 All employees, agents, contractors, or other parties working on behalf of the Company handling employee personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to employee personal data, whether in the workplace or otherwise;

32.7 Methods of collecting, holding, and processing employee personal data shall be regularly evaluated and reviewed;

32.8 All employee personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

32.9 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling employee personal data shall be regularly evaluated and reviewed;

32.10 All employees, agents, contractors, or other parties working on behalf of the Company handling employee personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

32.11 All agents, contractors, or other parties working on behalf of the Company handling employee personal data must ensure that any and all of their employees who are involved in the processing of employee personal data are

held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;

32.12 Where any agent, contractor or other party working on behalf of the Company handling employee personal data fails in their obligations under this Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

33. Sharing Personal Data

33.1 The Company may only share employee personal data with third parties if specific safeguards are in place.

33.2 Employee personal data may only be shared with other employees, agents, contractors, or other parties working on behalf of the Company if the recipient has a legitimate, job-related need-to-know. If any employee personal data is to be shared with a third party located outside of the European Economic Area, the provisions of Part 36, below, shall also apply.

33.3 Where a third-party data processor is used, that processor shall process personal data on behalf of the Company (as data controller) only on the written instruction of the Company.

33.4 Employee personal data may only be shared with third parties in the following circumstances:

a) the third party has a legitimate need to know the information for the purpose of providing services to the Company under a contract;

b) the sharing of the employee personal data concerned complies with the privacy notice provided to the affected employee data subjects (see Part 15 for more information) and, if required, the employees concerned have consented to the sharing of their personal data;

c) the third-party recipient has agreed to comply with all applicable data security standards, policies, and procedures, and has put in place adequate security measures to protect the employee personal data;

d) (where applicable) the transfer complies with any cross-border transfer restrictions (see Part 36, below); and

e) a fully executed written agreement containing GDPR-approved third party clauses has been entered into with the third-party recipient.

34. Transferring Personal Data to a Country Outside the EEA

34.1 The Company may from time to time transfer ('transfer' includes making available remotely) employee personal data to countries outside of the EEA.

34.2 The transfer of employee personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) the transfer is made with the informed and explicit consent of the relevant employee data subject(s);

d) the transfer is necessary for the performance of a contract between the employee data subject and the Company (or for pre-contractual steps taken at the request of the employee data subject);

e) the transfer is necessary for important public interest reasons;

f) the transfer is necessary for the conduct of legal claims;

g) the transfer is necessary to protect the vital interests of the employee data subject or other individuals where the employee data subject is physically or legally unable to give their consent; or

h) the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

35. Data Breach Notification

35.1 All personal data breaches concerning employee personal data must be reported immediately to the Company's Data Protection Officer.

35.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

35.3 If a personal data breach occurs and that breach is likely to result in a risk to

the rights and freedoms of employee data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

35.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 37.3) to the rights and freedoms of employee data subjects, the Data Protection Officer must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.

35.5 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

36. Implementation of Policy

This Policy shall be deemed effective as of 20/09/2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: James Doherty

Position: Director

Date: 01/01/2026

Due for Review by: 01/01/2027

Signature: