Personal Data Protection Policy

Incorporating the General Data Protection Regulation (GDPR)

1. Introduction

This Policy sets out the obligations of Owen Fabrications Ltd, a company registered in England under the CRN 04142278, who registered office is located at Yard 1, 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 regulation2016/679 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).

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 the 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.**

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, and his email address is 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 hold 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;

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:

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 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.

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 implementi8ng 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).

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 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.

16.2 Employees wishing to make an SAR should do so 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 he 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 the Company to 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 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 renumeration 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 the 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 the 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 at 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 with the GDPR's definition of special category.

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 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;

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 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 I 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 consultation either by the public in general, or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down by union or member state law for consultation are fulfilled in the particular case.

Name: James Doherty

Position: Director

Date: Wednesday 17th March 2021

Signature: 

Reviewal Date: Wednesday 16th March 2022