Olwg Ltd
Unit 1 The Factory
Catherine Wheel Road
Brentford
TW8 8BD

Subject: **Olwg Ltd Data Protection and Data Security Policy**

Ref.: POL-001

Issue Date: 12th March 2021

Prepared By:	Rosie Griffiths
Approved By:	Tony Griffiths
Next Review Date	12-03-22

Statement and purpose of policy

A. Olwg Ltd ("employer", "company", "we", "our", us") is committed to ensuring that all personal data handled by us will be processed accordingly to legally compliant standards of data protection and data security.

B. We confirm for the purposes of data protection laws that the employer is a data controller in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal data is processed.

C. The purpose of this policy is to help us achieve our data protection and data security aims by:

   i. Notifying our staff of the types of personal data that we may hold about them, our customers, suppliers and other third parties and what we do with that information;

   ii. Setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring that staff understand our rules and the legal standards; and

   iii. Clarifying the responsibilities and duties of staff in respect to data protection and data security.

D. This is a statement of policy only and does not form any part of any contract. We may amend this policy at any time in our absolute discretion.

E. For the purposes of this policy:

   i. Data protection laws means all applicable lows relating to the processing of Personal Data, including for the period during which it is in force, the UK General Data Protection Regulation (GDPR)

   ii. Data subject means the individual to whom the personal data relates.

   iii. Personal data means any information that relates to an individual who can be identified from that information.

iv. Processing means any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

v. Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Data Protection Principles

1. Staff whose work involves personal data relating to staff or others must comply with this policy and with the following data protection principles which require personal information which is:
    a. Processed lawfully, fairly and in a transparent manner. We must always have a lawful basis to process personal data, as set out in data protection laws. Personal data may be processed as necessary to perform a contract with the data subject, to comply with a legal obligation which the data controller is the subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. The data subject must be told who controls the information (us), the purpose (s) for which we are processing the information and to whom it may be disclosed.
    b. Collected only for specified, explicit and legitimate purposes. Personal data must not be collected for one purpose and then used for another. If we want to change the way we use personal data, we must first tell the data subject.
    c. Processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing. We will only collect personal data to the extent required for the specific purpose notified to the data subject.
    d. Accurate and the Company takes all reasonable steps to ensure that information is inaccurate is deleted or rectified without delay. Checks to personal data will be made when collected and regular checks must be made afterwards. We will make reasonable efforts to rectify or erase inaccurate information.
    e. Kept only for the period necessary for processing. Information will not be kept longer than it is needed an we will take all reasonable steps to del4ete information when we no longer need it. Contact us for guidance on how long particular information should be kept.
    f. Secure and appropriate measures adopted by the company to ensure as such.

Who is responsible for data protection and security

2. Maintain appropriate standards of data protection and data security is a collective task and shared between you and us. This policy and the rules contained in it apply to all staff of the Company, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers.
3. Contact us for any questions about this policy or requests for further information.
4. All staff have a personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that the measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. We must be notified if this policy has not been followed as soon as reasonable practicable.
5. Any breach pf this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing staff or customer personal data without authorisation or legitimate reason to do so may constitute gross misconduct and could lead to dismissal without notice.

What personal data and activities are covered by this policy.

6. This policy covers personal data:
    a. Which relates to a natural living individual who can be identified either from that information in isolation or reading it together with the information we possess.
    b. Is stored electronically or on paper in a filing system;
    c. In the form of statements of opinion as well as facts;
    d. Which relates to staff (present, past or future) or to any other individual whose personal data we handle or control;
    e. Which we obtain, or is provided to us, which we hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy;
7. This personal data is subject to the legal safeguards set out in the data protection laws.

What personal data do we process about staff?

8. We collect personal data about you which:
    a. You provide or we gather before or during your employment or engagement with us;

b. Is provided by third parties, such as references or information from suppliers or another party that we do business with; or
c. Is in the public domain.

9. The types of personal data that we may collect, store and use about you include records relating to your:
    a. Home address, contact details and contact details for your next of kin;
    b. Recruitment (including your application form or curriculum vitae, references received and details of your qualifications);
    c. Pay records, national insurance number and details of taxes and any employment benefits such as pension and health insurance (including details of any claims made);
    d. Telephone, email, internet or fax or instant messenger use;
    e. Performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.

Sensitive personal data

10. We may from time to time need to process sensitive personal information (sometimes referred to 'special categories of personal data');
11. We will only process sensitive information if:
    a. We have a lawful basis for doing so, e.g. it is necessary for the performance of the contract;
    b. One of the following special conditions for processing personal information applied:
        i. The data subject has given explicit consent;
        ii. The processing is necessary for the purposes of exercising the employment law rights or obligations of the company of the data subject;
        iii. The processing is necessary to protect the data subjects vital interests, and the data subject is physically incapable of giving consent;
        iv. Processing relates to personal data which are manifestly made public by the data subject;
        v. The processing is necessary for the establishment, exercise or defence or legal claims; or
        vi. The processing is necessary for reasons of substantial public interest.

12. Before processing any sensitive personal information, you must inform us of the proposed processing in order for us to assess whether the processing complies with the criteria noted above.
13. Sensitive personal information will not be processes until the assessment above has taken place and the individual has been properly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
14. Our privacy notice sets out the type of sensitive personal information that we processes, which it is and the lawful basis for the processing.

How we use your personal data

15. We will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our privacy notice. We will not process personal information for any other reason.
16. In general we will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including, but not limited to:
    a. Address list: to compile and circulate lists of home addresses and contact details to contact you outside working hours;
    b. Sickness records: to maintain a record of your sickness absences and copies of any doctors notes or any other documents supplied to us in connection with health to inform your colleagues that you are absent through sickness, as reasonable necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence level, to publish internally aggregated, anonymous details of sickness absence.
    c. Monitoring IT systems :to monitor your use of email, internet and telephone, computer or other communications or IT resources.
    d. Disciplinary, grievance or legal matters: in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.
    e. Performance reviews: to carry out performance reviews.
    f. Equal opportunities monitoring: to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of our workforce.

Accuracy and relevance

17. We will

a. Ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.
b. Not process personal data obtained for one purpose for any purpose, unless you agree to this or reasonably expect this.

18. If you consider that any information held is about you or is inaccurate or out of date, then you should tell us. If we agree that the information is inaccurate or out of date then we will correct it promptly. If we do not agree with the correction we will note your comments.

Storage and retention

19. Personal date (and sensitive personal information will be kept securely in accordance with this policy.
20. Periods for which we hold personal data are contained in our privacy notices.

Individual Rights

21. You have the following rights in relation to your personal data.
22. Subject access requests:
    a. You have the right to make a subject access request. If you make a subject access request we will tell you:
        i. Whether or not your personal data is processed and if so why the categories of personal data concerned and the source of the data if it is not collected from you;
        ii. To whom your data is or may be disclosed;
        iii. For how long your personal data is stored (or how that period is decided);
        iv. Your right of rectification or erasure of data or to restrict or object to processing;
        v. Your right to complain to the information commissioner if you thing we have failed to comply with your data protection rights; and
        vi. Whether or not we carry out automated decision-making and the logic involved in any such decision making.
    b. We will provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically unless we agree otherwise.
    c. To make a subject request, contact us at info@olwg.co.uk.
    d. We may need to ask for proof of identification before your request can be processed. We will let you know if we need to verify your identify and the documents we require.

e. We will normally respond to your request as quickly as possible. We will advise if a delay is expected.

f. If your request is manifestly unfounded or excessive we are not obliged to comply with it.

23. Other rights:

a. You have a number of other rights in relation to your personal data. You can require us to:

i. Rectify inaccurate data;

ii. Stop processing or erase data that is no longer necessary for purposes of processing;

iii. Stop processing or erase data if your interests override our legitimate grounds for processing data (where we rely on our legitimate interests are a reason for processing data);

iv. Stop processing data for a period if data is inaccurate of there is a dispute about whether or not your interests override our legitimate grounds for processing the data.

v. To request that wea take any of these steps, please sent the request to, info@olwg.co.uk.

Data Security

24. We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

25. Maintaining data security means making sure that:

a. Only people who are authorised to use the information can access it;

b. Where possible, personal data is pseudonymised or encrypted;

c. Information is accurate and suitable for the purpose for which it is processed; and

d. Authorised persons can access information if they need it for authorised purposes.

26. By law we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining and destroying the information.

27. Personal information must not be transferred to any person to process (e.g. while performing services for us or on our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

28. Security procedures include:
    a. Any desk or cupboard containing confidential information must be kept locked;
    b. Computers should be locked with a strong password that is changed regularly or shut down when left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others;
    c. Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when not being used.
    d. The directors must approve of any cloud used to store data.
    e. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
    f. All servers containing sensitive personal data must be approved and protected by security software.
    g. Servers containing personal data must be kept in a secure location away from general office space.
    h. Data should be regularly backed up.
29. Telephone Precautions: particular care should be taken when dealing with telephone enquiries to avoid inappropriate disclosures. In particular:
    a. The identity of the telephone caller must be verified before any personal data is disclosed;
    b. If the callers identity cannot be verified satisfactorily then they should be asked to put their query in writing;
30. Methods of disposal. Copies of personal information, whether on paper or any physical storage device must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks must be rendered permanently unreadable.

Data Impact Assessments

31. Some of the processing we carry out may result in risks to privacy.
32. When processing would result to high risks to rights and freedoms we will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

33. If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals we will report it to the Information Commissioner within 72 hours of discovery.
34. We will record all data breaches regardless of their effect.
35. If the breach is likely to result in high risk to your rights and freedoms we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

Individual Responsibilities

36. Everyone is responsible for helping the company keep their personal data up to date.
37. You should let us know if personal data provided changes e.g. if you move house or change your bank details.
38. You may have access to the personal details of other employees and customers over the course of employment. Where this is the case, we rely on you to help us mees the data obligations to everyone.
39. Individuals who have access to personal data are required:
    a. To access only personal data that they authority to access and only for authorised purposes;
    b. Not to disclose personal data except to individuals (whether inside or outside of the company) who have appropriate authorisation;
    c. To keep personal data secure e.g. by complying with the rules on access to premises, computer access, including password protection, and secure file storage and destruction;
    d. Not to remove personal data or devioces that can be used to access personal data from the companys premises without adopting appropriate security measures to secure the data and the device; and
    e. Not to store personal data on local drives or on personal devices that are used for work purposes.