Data Protection Policy

1. Introduction

This Policy sets out the obligations of Wyvern Business Systems Limited ("the Company") regarding data protection and the rights of clients, contractors, employees, agents and business contacts ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 natural person.

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 deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

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

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

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

d) accurate and kept up to date having regard to the purposes for which they are processed, is erased or rectified without delay;

e) 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;

f) processed in a manner that ensures appropriate security of the personal data.

3. Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a) Consent is given to the processing of his or her personal data for one or more specific purposes;

b) 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) for compliance with a legal obligation to which the controller is subject;

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

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

f) for the purposes of the legitimate interests pursued by the 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.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 The Company collects and processes the personal data set out in Part 13 of this Policy.

4.2 The Company only processes personal data for the specific purposes set out in Part 13 of this Policy. The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Accuracy of Data and Keeping Data Up To Date

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at 12 month intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that

data, as appropriate.

6. **Timely Processing**

The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it safely without delay.

7. **Secure Processing**

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8. **Accountability**

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

a) The name and details of the Company, its data protection officer if so appropriate, and any applicable third party data controllers;

b) The purposes for which the Company processes personal data;

c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data from the Company;

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

f) Details of how long personal data will be retained by the Company; and

g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

9. **Privacy Impact Assessments**

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation and it shall address the following areas

of importance:

9.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

9.2 Details of the legitimate interests being pursued by the Company;

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

9.4 An assessment of the risks posed to individual data subjects; and

9.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

10. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

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

e) The right to restrict processing;

f) The right to data portability;

g) The right to object;

h) Rights with respect to automated decision-making and profiling.

11. Keeping Data Subjects Informed

11.1 Any data gathered from our website will be subject to consent via our Privacy Notice. For all other data subjects when personal data is collected the following will be provided in our Terms and Conditions.

a) Details of the Company;

b) The purpose(s) for which the personal data is being collected and will be processed;

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

d) Where the personal data is not obtained directly from the data

subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties for example hosting, manufacturers and payroll providers;

f) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

g) Details of the data subject's rights under the Regulation;

h) Reference to the Data Subject Request Response Procedure setting out data subject's right to withdraw their consent to the processing of personal data, make a subject access, to complain to the Information Commissioner's Office;

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

12. Data Subject Access

12.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

12.2 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 a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

12.3 For full details please the Company's Subject Access Request Procedure which also includes reference to the following:

a) Rectification

b) Erasure

c) Restrictions

d) Objections

13. **Personal Data**

The following personal data may be collected, held, and processed by the Company:

a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses

b) information/documents provided from you in order to sustain the contract

c) Warranty and Insurance details

d) History of correspondence with Wyvern Business Systems Ltd

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

e) Where we need to perform the contract we have entered into with you.

f) Where we need to comply with a legal obligation.

g) Products, Offers and Services if opted in to receive communication from ourselves

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Wyvern Business Systems Ltd will not transfer or sell to any third party for marketing purposes, and data it holds relating to student under any circumstances.

14. **Data Security – Disposal**

When any 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 Information Security and Data Retention Policy.

15. **Data Protection Measures**

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All emails containing personal data must be encrypted

b) Where any 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. Hardcopies should be shredded, and electronic copies should be deleted securely.

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

d) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the forthcoming transmission;

e) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient;

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

g) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked drawer, cabinet or office;

h) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, family or other parties including the general public at any time;

i) If 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;

j) No personal data should be transferred to any device personally belonging to an employee and 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 the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

k) All personal data stored electronically should be backed up every 24 hours with backup's stored offsite.

l) All electronic copies of personal data should be stored securely using passwords and data encryption;

m) All passwords used to protect 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.

n) 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.

16. Organisational Measures

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

a) 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 the Regulation and under this Policy, and shall be provided with a copy of this Policy;

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

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

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

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or

other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

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

h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;

i) Where any agent, contractor or other party working on behalf of the Company handling 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.

17. Data Breach Notification

17.1 All personal data breaches must be reported immediately to Dan Rowbottom (Operations Manager)

17.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer, if so appropriate, 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.

17.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, Dan Rowbottom (Operations Manager) must ensure that all affected data subjects are informed of the breach directly and without undue delay.

17.4 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, if so appropriate (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.