Data Protection Policy	
Document:	**DatProtPol/002**
Compiled By:	**Paul Ashworth & Michell Watson**
Issue:	**2**
Date:	**01/12/2018**

DATA PROTECTION POLICY

The General Data Protection Regulation (GDPR) 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.

Personal Data

The Company holds personal data that is directly relevant to its employees. That personal data shall be collected, held, and processed in accordance with employee data subjects' rights and the Company's obligations under the GDPR and with this policy. The Company may collect, hold, and process personal data such as that detailed below:

- Identification information relating to employees such as names and contact details
- Equal opportunities monitoring information (such information shall be anonymised where possible) such as age, gender, ethnicity, religion etc.
- Health / medical records such as absence details, medical conditions, disabilities, medication and allergies.
- Employment information, such as; interview notes, CV's, performance reviews, disciplinary records, salary information, grievance information

Please note, this list is not exhaustive.

The Company will only collect and process 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).

Special Category Data

If the personal data in question is special category data (also known as sensitive personal data), e.g. data concerning the data subject's race, ethnicity, politics, religion, trade union membership,

genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation, at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes
- 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
- 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

The Processing of Personal Data

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

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- 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 with them
- The processing is necessary for compliance with a legal obligation to which the data controller is subject
- The processing is necessary to protect the vital interests of the data subject or of another natural person
- 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
- 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.

Accuracy of Data

The Company shall ensure that all 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

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any 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.

Secure Processing

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

Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of employee data subjects under the GDPR.

Rectification of Personal Data

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

The Company shall rectify the 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.

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

Erasure of Personal Data

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

- It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The employee data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- 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)
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless the Company has reasonable grounds to refuse to erase 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.

In the event that any 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).

Restrictions and Objections to Personal Data Processing

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

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.

In the event that any affected 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).

Subject Access Request Procedure

Data subjects may make a subject access request (SAR) 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.

Data subjects wishing to make a SAR may do so in writing, using the Company's SAR form. Responses will be provided within a month of receiving the SAR. If the SAR is complex or numerous requests are made this time may be extended, in which case the individual will be notified.

No fee will be charged for a SAR, however, charges may be made for additional copies of information provided or if requests are deemed to be excessive.

The Company is able to decline a SAR if it is unreasonable, excessive or unfounded.