**GENERAL DATA PROTECTION REGULATION (GDPR) POLICY**

MAY 2018

**Purpose**

Daniel Thwaites Plc ("the Company") operates the following policy in relation to data protection. This policy applies to all employees of the Company.

Principles

The Company is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees. This policy sets out how the Company deals with personal data, including personnel files and data subject rights, and employees' obligations in relation to personal data.

**Processing of Personal Data**

The Company will process Personal Data in accordance with the following EIGHT DATA PROTECTION PRINCIPLES:

1. fairly and lawfully;
2. for specified, explicit and legitimate purposes;
3. where it is adequate, relevant and not excessive;
4. will ensure accuracy and will take all reasonable steps to ensure inaccurate personal data is rectified or deleted without delay;
5. not keep longer than is necessary;
6. process in accordance with individuals' rights;
7. keep secure; and
8. not transfer to countries without adequate protection.

The Policy applies only to information that constitutes "personal data". Information is "personal data" if it:

* identifies a person or information relating to a person that we can identify from that data whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
* is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

This Policy applies to all Personal Data we process regardless of the media on which the data is stored (on paper, computerised systems, including email and social media)

**The Use of Personal Data**

Personal Data will only be collected for specified, explicit and legitimate purposes. It will not be further processed in any manner incompatible with those purposes.

Personal Data will not be used for new, different or incompatible purposes without first informing the employee and gaining consent where necessary.

"Sensitive personal data" is information about an individual's:

* racial or ethnic origin;
* political opinions;
* religious beliefs or other beliefs of a similar nature;
* trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
* physical or mental health or condition;
* sex life;
* commission or alleged commission of any criminal offence; and
* proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Company will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. If the Company enters into discussions about a merger or acquisition with a third party, we will seek to protect employees' data in accordance with the data protection principles.

**Personnel Files**

An employee's personnel file is likely to contain information about their work history and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

There may also be other information about the employee located within the Company, for example in their line manager's inbox or desktop; with payroll, or within documents stored in a relevant filing system.

The Company will ensure that personal information about an employee, including information in personnel files, is securely retained. Any hard copies of information will be stored in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

**Data Subject Rights**

Under certain circumstances, by law, an employee has the right to:

Request Access to personal information (known as Data Subject Access Request). This enables the employee to receive a copy of the personal information held. The Company will respond to any Data Subject Access Request within 30 days.

Request Correction of personal information that the Company holds about the employee, if it is believed the information is incomplete or inaccurate.

Request erasure of personal information. This enables the employee to ask the Company to delete or remove personal information where there is no good reason for the Company continuing to process it.

Object to processing of personal information.

Request the restriction of processing of personal information.

Request the transfer of personal information to another party.

Any such requests should be made via the Company’s Data Protection Officer, Mrs. Susan Woodward.

The Company may reserve its right to withhold the employee's rights where any statutory exemptions apply.

**Monitoring**

The Company may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. Should this take place, employees will be made aware.

**Employees' Obligations Regarding Personal Information**

If an employee acquires any personal information in the course of their duties, they must ensure that:

* the information is accurate and up to date, insofar as it is practicable to do so;
* the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
* the information is secure at all times i.e. if paper files, laptops, personal devices are taken off site, they must not be left unattended e.g. in vehicles

In particular, an employee should ensure that they:

* use password-protected and encrypted software for the transmission and receipt of emails;
* send fax transmissions to a direct fax where possible and with a secure cover sheet; and
* lock files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, they must inform the Data Protection Officer immediately.

**Consequences of Non-Compliance**

All employees are under an obligation to ensure that they have regard to the eight data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal.