Colloide

General Data Protection Regulations (GDPR) Policy
CES IMS-POL4

Status: Ratified

Document Type: Policy

T: 028 8675 8638 I E: info@colloide.com I www.colloide.com

Document Control Sheet

Date	Rev	Amended By	Comments/Details
01/08/2019	1	P McGuinness	First Issue
14/10/2020	2	P McGuinness	Annual Review
14/10/2021	3	P McGuinness	Updated to New Format
17/10/2022	4	P McGuinness	Annual Review

Policy & Procedures
This document sets out the Company's policies in relation to data protection and aims to set out Company expectations of employees, and what employees can expect of the organisation when obtaining, maintaining, processing, and destroying personal data.

Colloide recognise the importance of complying with the Data Protection Act 2018 which places obligations upon employers and employees who hold data about employees and other individuals. This applies to all current, past, and temporary staff. All personnel involved in holding confidential or personal information should note that it is illegal to pass on, misuse or not secure any such records.

GDPR Principles
Colloide operates to comply fully with the Data Protection Act and its data protection principles. The following principles set the framework upon which data processing activities within the organisation are conducted. As such, all personal data (including employees and third parties) must:

- Be processed lawfully, fairly and in a transparent manner.

- Be collected for a specific, explicit, and legitimate purpose and not further processed in a manner which is incompatible with that purpose; further processing for archiving purposes in public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Be adequate, relevant, and limited for what is necessary in relation to the purposes for which it is processed.

- Be accurate and where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, and rectified without delay

- Be kept in a form which permits identification of data subjects (individuals whose personal data is being used) for no longer than is necessary for the purposes for which the personal data are processed

- Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Types of Information Held
The purpose for which we obtain, maintain, and destroy any personal information is for use solely for administrative and personnel management purposes; including but not limited to:

- Recruitment
- Appraisals and performance management
- Promotion

- Training & career development
- Pay and remuneration
- Pension and insurances and other benefits
- Tax, national insurance and other deductions from pay
- Health and safety
- Discipline and grievances
- Review of our human resources policies.
- Correspondence with the Company and other information provided to the Company by other organisations

Sharing of Information
From time to time we may need to disclose information to relevant third-party companies (e.g., where we are legally obliged to do so or where we are requested by an employee to provide a reference).

It should also be noted that the Company may hold information about employees for which disclosure will be made only when strictly necessary; this could include for example, information about an employee's health, for the purpose of compliance with our Health and Safety and our Occupational Health obligations.

Information provided by other organisations and shared with the Company will be obtained and held for the purposes defined in between both parties and as stated in the contract. Data will only be held for as long as required to fulfil the purpose.
In such instances, where we are required to share your information, you will be informed in advance.

Employee Responsibilities
Training will be given on the requirements of the GDPR; employees are required to complete all assigned data protection training as requested.

As an employee, you must adhere to the following responsibilities at all times during the course of your employment:

- Understand your data protection obligations fully and make sure that you are continuously mindful of these throughout the course of your employment activities.
- Ensure that all data processing activities you are undertaking comply with our procedures and are justified.
- Do not use data in any unlawful manner or in any manner which contradicts this policy.
- Store all data correctly, all data should be kept secure and protected from any unlawful processing and against accidental loss or destruction.
- You should hold data for the required length of time only and in light of the purposes for which that data was originally collected, held, and processed.
- Comply with this procedure at all times.
- If you become aware of any data breaches or near misses or if you have any concerns relating to data, you must raise this immediately with the Data Protection Officer (DPO)

or equivalent or a member of management. You should be vigilant regarding information and report anything which is contradictory to Company procedures.

Subject Access Request
If you wish to access the personal data which we hold about you, you must make a request in writing to your Data Protection Officer (DPO) or equivalent. There will be no fee for making a subject access request, however in instances whereby requests are excessive and or repetitive, an administration fee may be applied.

We will respond to your request without delay and at latest, within one month of receiving the written request. If necessary, this timescale can be extended by a further two months if the request is complex. However, you will be contacted within one month of the receipt of the request and we will explain why an extension is necessary in this instance.

We will endeavour to provide the information in a commonly used electronic format. Some information may be exempt from subject access requests, in such instances, your Data Protection Officer (DPO) or equivalent will explain the reasons why this request will not be carried out.

Reporting Breaches
Any breach or contradiction of this policy or GDPR must be reported immediately upon becoming aware of a breach or concerns. The Company has a legal obligation to report data breaches to the ICO within specific timeframes, which are set by the ICO.

Any member of staff who fails to notify a breach or is found to have known or suspected a breach has occurred but has not followed the Company procedure and reporting procedures outlined above, will be dealt with in accordance with the Company's Disciplinary Procedure.

Failure to Comply
The Company deems compliance of this procedure with the utmost importance in all areas of our business. Failure to comply puts not only employees but also the Company at risk.

Failure to comply could make an employee liable for disciplinary action, which could lead to dismissal as reflected in the Company's Disciplinary Policy.

If you have any questions about this procedure or require further guidance/training, do not hesitate to contact your Line Manager. The Data Protection Officer (DPO) or equivalent is responsible for overseeing the Company's data protection strategy and implementation to ensure that overall compliance is met.

To achieve compliance with the above, Colloide ensure that:

- We have individuals within Colloide who can provide advice and assistance on issues in relation to the Data Protection Act
- Anyone handling and managing personal information understands that they are responsible for following Data Protection Principles.
- Procedures for handling personal information are clearly described and established.

- Regular reviews of managing personal data.

Data protection compliance principally rests with Colloide; however, every employee has an individual responsibility to ensure compliance and can be held legally accountable.

SIGNED BY: 

Date Reviewed: **17th October 2022**

Date of Next Review: **17th October 2023**