# MELTON COLLEGE

# Data Protection Policy

The organisation is committed fully to compliance with the requirements of the General Data Protection Regulation (GDPR). The GDPR applies to all organisations that process data about their employees, as well as others, e.g., customers and clients. It sets out principles which should be followed by those who process data, and it gives rights to those whose data is being processed.

To this end, the organisation endorses and adheres fully to observing the eight individual rights set out under the GDPR, these are the following.

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision-making and profiling.

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the organisation will:

- observe fully the conditions regarding having a lawful basis to process personal information.
- meet its legal obligations to specify the purposes for which information is used.
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs, protect legitimate interests or to comply with any legal requirements.
- ensure the information held is accurate and up to date.
- ensure that the information is held for no longer than is necessary.
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information.

- ensure that personal information is not transferred outside the EU, to third countries or international organisations without an adequate level of protection.

**Status of this Policy**

The policy does not form part of the formal contract of employment for employees, but it is a condition of employment that employees will abide by the rules and policies made by Melton College from time to time. Any failure to follow the Data Protection Policy may, therefore, lead to disciplinary proceedings. This policy was approved on 25 May 2021 It will be reviewed no later than 25 May 2022.

**Designated Data Protection Officer**

The Designated Data Protection Officer, The College Manager, will deal with day-to-day matters. Any member of staff or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the Designated Data Protection Officer.

**Staff Responsibilities**

All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date.
- informing the organisation of any changes to information that they have provided, e.g., changes of address, either at the time of appointment or subsequently — the organisation cannot be held responsible for any errors unless the employee has informed it of such changes.

**Data Security**

All staff are responsible for ensuring that:

- any personal data that they hold is kept securely.
- personal information is not disclosed either orally or in writing, or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it must be coded, encrypted or password-protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

**Subject Consent**

Consent is one lawful basis for processing, and consent (or explicit consent) can also legitimise use of special category (sensitive) data, restricted processing and overseas transfers of data.

Subject consent will have to be explicit, in relation to each processing activity, and freely given. Consent will not be freely given if there is imbalance in the relationship between the individual and the data controller — this will make consent particularly difficult for employers, who should look for an alternative lawful basis where possible.

Employers will not be able to rely on a generic reference to consent within an employment contract or data protection policy, which an employee is required to agree as part of wider terms and conditions. Consent must be capable of being easily withdrawn by the employee at any time, this means employers need to have simple and effective withdrawal mechanisms in place.

Where relying on consent to process personal data, being able to prove how consent was obtained will be vital for employer compliance with the GDPR.

**Subject Access**

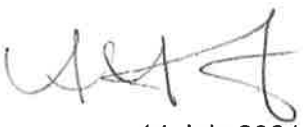
An employee may submit a written request for details of personal information which the company holds about him or her under the GDPR free of charge. If an employee would like a copy of the information held on him or her, he or she should write to or email Andrew Hjort, Principal, Melton College, 137 Holgate Road, York, YO24 4DH. The requested information will normally be provided within one month of receipt of the request. If the request is made electronically, the information will be issued in an electronic format. It is possible to extend the period of compliance by a further two months where requests are complex or numerous.

A reasonable fee may also be charged to comply with requests for further copies of the same information. This does not mean that a charge for all subsequent access requests will be made. The fee must be based on the administrative cost of providing the information.

If an employee believes that any information held on him or her is incorrect, incomplete or out of date, then he or she should write to or email Andrew Hjort as soon as possible, at the above address. The organisation will promptly correct any information found to be incorrect and respond within one month to the request for rectification. This time limit can be extended by two months where the request for rectification is complex.

**Conclusion**

This policy sets out this organisation's commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

Signed: 

Date: 14 July 2021

Policy review date: 14 July 2022