Data Protection Policy

A) INTRODUCTION

Mercia College Limited controls and processes the personal data of staff, students and to a lesser extent visitors, contractors and suppliers. This policy is designed to ensure that Mercia College Limited complies with the law. The UK Data Protection Act of 1998 (DPA) is being replaced by the General Data Protection Regulation (GDPR) on 25th May 2018. The new regulation carries a legal obligation to protect the fundamental rights of individuals when their personal data is outside their control and could lead to their privacy being compromised. A new data protection bill is currently passing through parliament this will supplement GDPR. The new bill will update the rights of individuals to make them easier to exercise and to ensure they continue to be relevant in the face of rapidly changing technology.

Personal data is defined as any information relating to an identified or identifiable natural living person. That is identifiable directly or indirectly for example a CCTV image, an email address that identifies the individual, an ID number or name and DOB.

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, student, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

B) DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

C) THE RIGHTS OF DATA SUBJECTS

All data subjects (staff, students, visitors and other whose personal data is held by Mercia College) have the following rights:

The right to be informed. Individuals have the right to be informed about the collection and use of their personal data, this is a key transparency right under GDPR. Data subjects must be provided with information including; Mercia College's purpose for processing their personal data, retention periods for that personal data, and who it will be shared with. This is called 'privacy information' and must be provided to individuals at the time Mercia College collects their personal data from them

Senior managers listed in paragraph must ensure privacy information is concise, transparent, intelligible, easily accessible, and it must use clear and plain language. Privacy information must be regularly reviewed, and where necessary, updated. Any new uses of an individual's personal data must be brought to their attention before you start the processing.

The right of access. Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed, access to their personal data and other supplementary information, (this is normally provided in the privacy statement). Such subject access requests (SAR) must be sent to the Data Protection Officer and data provided within 1 calendar month. Mercia College cannot charge for this service except in rare circumstances refer to GDPR guidelines https://ico.org.uk/for-organisations/guide- to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

An individual can make a request for rectification, erasure, and restricted processing verbally or in writing. Mercia College has one calendar month to respond to a request. All requests must be recorded and a response to the individual given. Senior managers must ensure they have a system for recording requests and responses to these rights. Managers must ensure that staff are briefed on how to handle such requests

The right to rectification. Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. There are situations where it may not be possible to rectify data for guidance see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

The right to erasure. Individuals have the right for personal data erased, also known as 'the right to be forgotten'. The right to erasure does not apply if processing is necessary for example: to comply with a legal obligation. Managers must check the ICO website before refusing to erase data. https://ico.org.uk/for-organisations/guide-to- the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

The right to restrict processing. Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right, when processing is restricted, Mercia College is permitted to store the personal data, but not use it. Managers must check the ICO website if refusing the right to rectification. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

There are 3 further rights; the right to data portability, the right to object and rights in relation to automated decision making and profiling. Any requests from individuals invoking these rights must be referred to the data protection officer.

D) RESPONSIBILITIES OF STAFF AND STUDENTS

All members of staff and students are responsible for:

a. Checking that any information that they provide to Mercia College in connection with their employment or enrolment is accurate and up to date.
b. Informing Mercia College of any changes to information, which they have provided,
e.g. change of address

E) DATA SECURITY STAFF RESPONSIBILITIES

All members of staff are responsible for ensuring that:

Any personal data which they hold is kept securely.

Personal information is not disclosed either orally or in writing or 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.

Staff must report data breaches to the DPO without delay.

Other than for emergencies where next of kin data can be used, parents of students aged over 18 must not be contacted unless we have the permission of the young person recorded centrally and the permission of the parent also recorded centrally, unless there are issues around the student's competency to understand key matters and the Mercia College needs to consult a parent, guardian or social worker

Personal information should be kept in central systems such as the MIS, HR, ILP & tracking, finance and supported learning systems. Staff should not keep personal data in their own spreadsheets, databases or other application software. If the data needs to be printed great care must be taken to ensure only those authorised to see such data are able to. Where possible such data should be anonymised.

Where central systems do not support the processes needed this must be recorded as outlined in paragraph 6. Such data must not be shared via email unless encrypted. Staff are encouraged to share data via Office 365 which is secure.

All company owned mobile devices and any USBs used in the company must not be used to store personal data.

Great care must be taken when transporting or accessing personal data outside of the company premises whether this is held on paper on mobile devices. Personal data must not be left in public places or accessed in places where you could be overlooked. Password controlled screen savers must be used.

Paper records must be kept in locked filing cabinets or drawers. In some cases such as HR and supported learning managers of those areas should regularly review the need to restrict entry.

Teaching staff who hold personal information such as course work and exam results must ensure these are kept securely in locked filing cabinets or desk drawers and confidentiality is maintained.

F) ORGANISATIONS AND OTHERS TO WHICH MERCIA COLLEGE MAY PROVIDE DATA

Mercia College may provide data relating to staff and students to organisations, including but not limited to, Government Departments including the Department for Education, HMRC, the disclosure and barring service, the Funding Councils (including the Education and Skills Funding Agency, and the Higher Education Funding Council for England), Local Education Authorities, Student Loans Company, Awarding Organisations, Sub

Contractors, Universities, Police, auditors, pension providers, and, for those receiving benefits, the Department for Work and Pensions. It may also be the case that personal information is provided to such organisations through agencies acting on their behalf.

a. any employee benefits operated by third parties;
b. disabled individuals - whether any reasonable adjustments are required to assist them at work;
c. individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
d. for Statutory Sick Pay purposes;
e. HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f. the smooth operation of any employee insurance policies or pension plans;
g. to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

Where data is shared this must be clearly stated in the privacy information given to the data subject.

Where data is shared with a third party organisation Mercia College will ensure a signed data sharing contract is in place that ensures data processed complies with GDPR

G) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a. processing will be fair, lawful and transparent
b. data be collected for specific, explicit, and legitimate purposes
c. data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d. data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e. data is not kept for longer than is necessary for its given purpose
f. data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g. we will comply with the relevant GDPR procedures for international transferring of personal data

H) ACCESS TO DATA

As stated above, data subjects have a right to access the personal data that we hold on them. To exercise this right, Data subjects should make a Subject Access Request (SAR). We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

I) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

J) REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

K) TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

L) RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

M) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Keli Burns
Director
01332 332727