## Introduction

Middlesbrough College needs to keep certain information about its employees, learners and other people users to allow it to monitor performance, attendance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government met.

Our use of information is governed by the principles of the General Data Protection Regulation (GDPR). Under the regulations, personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are corrected or delated as appropriate.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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 organisational measures.

Middlesbrough College and all staff or others who process or use personal information must ensure that they follow these principles at all times.

## 2 Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Middlesbrough College from time to time. Failure to follow the Data Protection Policy can therefore result in disciplinary proceedings.

## 3 Notification of Data Held and Processed

All staff, learners and others are entitled to

- Know what information Middlesbrough College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what Middlesbrough College is doing to comply with its obligations under GDPR.

Middlesbrough College will therefore provide staff, learners and others with notification of the types of data Middlesbrough College holds and processes about them, and the reasons for which it is processed.

## 4 Responsibilities of Staff

All staff are responsible for

- Checking that the information they provide to Middlesbrough College in connection with their employment is accurate and up to date.
- Informing Middlesbrough College of changes to or errors in information held.
- If, as part of their responsibilities, staff collect information about other people e.g., about learners' course work, opinions about ability, references to other academic institutions, details of personal circumstances, they must comply with the guidelines for staff - see later.

## 5 Data Security

All staff are responsible for ensuring that

- Personal data they hold are kept securely.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party. Unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

- Any suspected data breaches are reported timely to the College Data Protection Officer (see Appendix 2).

Personal information should be

- Kept under lock and key when not attended.
- Must only be processed using approved, College provided systems.

## 6 Learner Obligations

Learners must ensure that all personal data provided to Middlesbrough College are accurate and up to date. They must ensure that changes of address, etc, are notified to the Registry and Finance department.

## 7 Rights to Access Information

Staff, learners and contractors have the right to access any personal data that Middlesbrough College keeps about them, either on a computer or in paper files.

Any person who wishes to exercise this right should contact Middlesbrough College Data Protection Officer 9see appendix 1 of this policy). Middlesbrough College can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. Middleborough College may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information. Please refer to the Subject Access Procedure for full details.

Middlesbrough College aims to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within one month of receipt of a completed subject access request form and accompanying information.

## 8 Subject Consent

Those who are offered places or posts at Middlesbrough College will be notified of the standard data kept about them, and the uses to which it may be put, as declared in our registration with the Information Commissioner. Acceptance of a place or a post will be understood to signify acceptance of such 'standard' processing.

Sometimes it is necessary to process 'sensitive' information, for instance, about a person's health, criminal convictions, race and gender or family. This may be to ensure that Middlesbrough College is a safe place to work or study, to operate Middlesbrough College policies e.g., sick pay, equal opportunities or to enable the institution to comply with the law. It is recognised that processing it may cause particular concern or distress to individuals so any reported data will be anonymised where possible. The college will seek consent to process sensitive information which is not specifically required for the provision of service, and opt-in consent for the data to be used for marketing purposes.

## 9 The Data Protection Officer and Data Owners

Middlesbrough College as a body corporate is the 'Data Controller' under GDPR, and the Governing Body is therefore ultimately responsible for implementation. The Data Protection Officer has been vested with day-to-day responsibility for implementing the provisions of this policy. The Data Protection officer is Paul Moody, Executive Director of Policy, Funding & Management Information.

The Data Protection Officer will ensure that the personal data held by the College is kept securely and used properly, within the terms of the regulations. The Data Protection Officer will inform college managers of any changes or amendments to GDPR and advise on the implementation of the regulations. Middlesbrough College has also designated 'Data Owners' responsible for files held in particular locations or for particular functions. Data Owners may designate authorised staff to process personal data.

Responsibility for day-to-day matters will be delegated to the Associate Directors / Assistant Principals / Vice Principals / Heads of Service / Principalship as designated Data Controllers. Information and advice about the holding and processing of personal information is available from the Data Protection Officer.

## 10 Retention of Data

Middlesbrough College will keep data for the minimum time necessary to fulfil its purpose and ensure effective disposal of any material no longer required. A full list of information with retention times is published and is available in the records retention and disposal policy.

## 11 Disposal of Data

The College will provide a secure system to dispose of confidential information with appropriate located reciprocals in all administration areas - these will be locked and will only be opened via the appointed contractor or the Estates Team.

## 12 Conclusion

Compliance with GDPR is the responsibility of all members of Middlesbrough College. Any deliberate breach of the Data Protection Policy may result in disciplinary action, access to facilities withdrawn, or even criminal prosecution. Questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

This policy should be read in conjunction with the following documents

- Records Retention & Disposals Policy.

## Responsibilities of Data Protection Officer

1 To be the nominated officer in the College's entry in the Data Protection Register.

2 To maintain the accuracy and currency of the College's registration with the Data Protection Registrar.

3 To administer processes for requests for information by data subjects exercising their rights under GDPR.

4 To advise staff on the provisions of GDPR and related legislation.

5 To devise and implement, along with other key managers, operational procedures for Middlesbrough College's compliance with GDPR.

6 To maintain the currency of the College's Data Protection Policy.

7 To report to CMT (College Management Team) on the College's compliance with the provisions of GDPR and related Acts regarding data and information.

## Responsibilities of Data Owners

1 To be responsible to the Data Protection Officer for the effective implementation of the College Data Protection Policy in respect of those records for which they are named "Data Owners".

2 To ensure that requests for information by data subjects exercising their rights under the regulations and forwarded by the Data Protection Officer are processed in accordance with the College's Data Protection Policy.

3 To identify staff who may process the data for which "Data Owners" are responsible and monitor them to ensure that processing complies with the College's Data Protection Policy.

4 To report to the Data Protection Officer when requested on their sections' compliance with the provisions of the College's Data Protection Policy.

## Staff Guidelines for Data Protection

1 GDPR covers any collection of data from which an individual may be identified. Under the regulations, "processing" such data means performing almost any action upon it: storing, amending, ordering, erasing, and so on. A designated "Data Protection Officer" is responsible for ensuring that the College fulfils its obligations under the regulations, and for implementing the College Data Protection Policy.

2 All staff process data about learners on a regular basis: when marking registers, writing reports or references, or as parts of pastoral or academic supervisory roles. Middlesbrough College will ensure through registration procedures that all learners give consent to this sort of processing and are notified of the categories of processing, as

required by the regulations. The information that staff deal with on a day-to-day basis will be "standard" and will cover categories such as

- General personal details like name and address.
- Details about class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

3 Information about a learner's physical or mental health, sexual life, political or religious views, Trade Union membership, ethnicity or race is "sensitive" and can only be collected and processed with the learner's express consent. e.g., recording information about dietary needs, for religious or health reasons prior to taking learners on a field trip, recording information that a learner is pregnant, as part of pastoral duties. If staff need to process such information, they must ensure that consent has been obtained and recorded appropriately.

4 **It is not always appropriate or sensible to give absolute assurances of confidentiality to those who may wish to talk about personal issues.** Staff at Middlesbrough College should deem confidential information as private to the institution, and not to themselves, as an individual employee.

Staff should make it clear at the onset of discussions with students, whether the content is to be confidential and the extent of the confidentiality to be afforded to any disclosures. In particular, they should inform the student of:

- The concern of the College to respect privacy, wherever possible.
- The circumstances, if any, under which information would be shared with a third party, taking account of the duty of care which may be owed to the individual and/or others; and the individuals or body who might be informed in such circumstances.
- The duties of the College under GDPR.

Staff involved in private discussions with students should, where possible, seek the consent of the individual for the onward disclosure of relevant information to those with a clear need to know. Where such consent is not forthcoming, the person entrusted with the information should make it clear that in exceptional circumstances, it may be necessary to disclose the information to others, whilst also making it clear that such disclosure would be on a need-to-know basis only, preserving strict confidentiality in relation to any third party.

5 Staff have a duty to make sure that they comply with the data protection principles, which are set out in the Data Protection Policy. In particular, staff must ensure that records are accurate, up-to-date, fair and kept and disposed of safely, in accordance with Middlesbrough College's Data Protection policy.

6 Middlesbrough College has designated some staff as “Data Owners”. Data Owners may authorise staff in certain areas to hold or process data that is sensitive, or not standard. Staff who are not so authorised may only process sensitive or non-standard data when they are satisfied that the processing of the data is necessary

- A - In the best interests of the learner or staff member, or a third person, or Middlesbrough College and if

- B - They have either informed the authorised person or have been unable to do so and processing is urgent and necessary. This should only happen in very limited circumstances: e.g., a learner is injured and unconscious, but in need of medical attention, and a tutor tells the hospital that the learner is pregnant.

The College must bear in mind that in certain circumstances they may owe a duty of care to individuals that cannot be discharged unless the institution takes action on information provided in confidence. It is not possible to provide an exact delineation of the extent of such duty of care. However, where, for example, withholding information could cause potential harm to an individual or to others, the College must weigh the duty of confidentiality against the potential risk to the individual and others.

7 Staff must not disclose personal data to any learner, unless for normal academic or pastoral purposes, without authorisation or agreement from the Data Protection Officer. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the Data Protection Officer.

8 Before processing any personal data, staff should consider the following checklist.

- Do you really need to record the information?

- Is the information “standard” or is it “sensitive”?

- If it is sensitive, do you have the data subject's express consent?

- Has the learner been told that this type of data will be processed?

- Are you authorised to collect/store/process the data?

- If yes, have you checked with the data subject that the data is accurate? Are you sure that the data is secure?

- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the learner or the staff member to collect and retain the data?

- Have you reported the fact of data collection to the authorised person within the required time?

## Definitions Relevant to Data Protection Policy

### Data

'Data' are any information

- Stored in a form capable of being processed by computer or other automatic equipment such as most computer files, including word processor, database and spreadsheet files.
- Recorded in any form for later processing by computer or other automatic equipment such as information collected from registration forms, CCTV pictures.
- Stored as part of a relevant filing system or intended to be included in one in the future including card files or filing cabinets structured by name, address or another identifier.
- Not covered by the above but part of an accessible record under GDPR such as a set of notes kept by a counsellor employed by the Middlesbrough College.

### Personal Data

'Personal data' are data that relate to a living individual who can be identified from that information, or from that data and other information in the possession of Middlesbrough College. These include any expression of opinion about the individual and of the intentions of Middlesbrough College in respect of that individual.

### Sensitive Personal Data

GDPR distinguishes between 'ordinary personal data' such as name, address and telephone number and 'sensitive personal data' including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions.

### Data Controller

The 'Data Controller' is Middlesbrough College and is so identified in Middlesbrough College's entry in the Data Protection Register.

### Data Protection Officer

The 'Data Protection Officer' is the nominated officer in Middlesbrough College's entry in the Data Protection Register. He or she is nominated by the Governing Body for the implementation of Middlesbrough College policies relating to the Data Protection Act and related Acts. The responsibilities of the Data Protection Officer are defined.

### Data Subject

A 'Data Subject' is any living individual who is the subject of personal data.

## Data Subject Access

'Data subject access' is the right of an individual to access personal data relating to him or her which is held by Middlesbrough College.

## Data Owner

A 'data owner' is a person authorised to manage the processing of data on behalf of Middlesbrough College.

## Processing

'Processing' includes technical operations on data, such as organisation, retrieval, disclosure, and deletion; but also obtaining and recording data; the retrieval, consultation or use of data; and the disclosure or otherwise making available of data.

## Appendix 1

## Subject Access Request Procedure

The General Data Protection Regulations (GDPR) entitles individuals to request access to any personal data that Middlesbrough College is holding about them. This is known as a Subject Access Request (SAR).

A SAR is where an individual (or a third party with their consent), using their rights under GDPR, makes a request for a copy of the personal data an organisation holds on them, or details of what data is held and its source.

SAR's can be made verbally, via email or in writing to Data Protection Officer (DPO), at the address below:
Middlesbrough College, Dock Street, Middlesbrough, TS2 1AD
Email: dpo@mbro.ac.uk

If a SAR is made verbally then the requester should be asked to put their request in writing, to allow the College to understand the nature of the SAR and to verify the identity of the requester.

Where a request is received elsewhere in the College, the Data Protection Officer should be immediately informed so they are able to deal with the request without delay.

Once the request is received the Data Protection Officer will confirm the identity of the requester and assess the scope of the request.

Details of the request and subsequent actions will be added to the Subject Access Request log.

Additional information may be requested to evidence the identity of the requester. This should be proportionate.

If a request is made by a person / organisation seeking the personal data of a data subject, and which purports to be made on behalf of that data subject, then should not be provided until it can be proved the data subject gave consent. The College should aim to reply to third party requests within 10 working days of receiving them in order not to delay unduly the process of returning any data.

The College will deal with a SAR free of charge, however, a fee may be charged in the following circumstances:

- Where a request is manifestly unfounded or excessive, or the College may refuse to respond to the request. The College will respond in writing stating their reasons for refusing to respond.
- Where a repeat request for the same information is made.

Written communication (via email or letter) should be sent to acknowledge receipt of or in the case of a third party to notify the subject of the request and ask for any additional information that may be needed.

Once the identity of the data subject (or the right/authority to request the data where the data subject is not the requester) the Data Protection Officer will begin the process of contacting the appropriate departments to collect and collate the information.

The DPO will take all reasonable and proportionate steps to identify and disclosure all data relating to the request.

To locate the correct information within the College, the DPO may ask the requester to confirm exactly what information they are requesting, or where they believe the information may be stored.

Where the information contains reference to third parties the DPO will redact the third parties. Where this is impossible and consent from the third party has not been received the information will not be disclosed.

The DPO will ensure that the information disclosed is clear and technical terms are clarified and explained.

The final response should be provided in a written format (via email or letter), including and as far as possible for what reasons, any data has been withheld.

The SAR will be responded to in one calendar month. This will run from the latter of:

- The date of the request.
- The date when any additional identification, or other information requested, is received.
- Payment of any required fee.

Any enquiries regarding this procedure or the Colleges Data Protection Policy should be directed to Middlesbrough College DPO, using details above.

## Appendix 2

## Personal Data Breach Procedure

This procedure outlines the Colleges response to Personal Data Breach incidents or suspected Personal Data Breach incident.

A Personal Data Breach is:

*"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".*

All persons who process personal data on behalf of the College are required to be aware of this procedure and are all responsible for:

- familiarising themselves with this procedure.
- promptly reporting any Personal Data Breaches or suspected breach to the college DPO.

As soon as a Personal Data Breach has been detected or is suspected the data user must report the incident as a matter of urgency to the Data Protection Officer at dpo@mbro.ac.uk, giving details of the breach or suspected breach.

A Personal Data Breach will be assessed and investigated by the Data Protection Officer (DPO). The DPO will examine: What was the sequence of events? What is the effect? What action has been taken and why? What is the situation now?

Details of the breach and subsequent actions will be added to the Personal Data Breach log.

For significant Personal Data Breaches involving a serious risk to the College and individuals whose data is involved, the Data Protection Officer may convene a response team consisting of relevant senior staff and/or seek external legal advice.

Digital Services will identify and implement without delay any IT actions required to learn more about and contain the Personal Data Breach and will regularly update the Data Protection Officer on the extent of the Personal Data Breach and progress on its containment.

The Data Protection Officer will identify other (non-IT) actions required to investigate and contain the Personal Data Breach. This may include:

- requesting further information from data users;
- asking data users to contact third parties to request return or deletion of personal data disclosed in error (and confirmation that such destruction has taken place;
- requiring passwords to be changed;
- attempted retrieval of devices/ documents;
- follow up / repeat attempts to contain the Personal Data Breach.

The Data Protection Officer, supported by the Senior Leadership Team, is responsible for deciding whether notification of a Personal Data Breach to the Information Commissioner's Office should be made by the College.

In accordance with data protection laws, notification must be made to the Information Commissioner's Office without undue delay and in any case within 72 hours of the College becoming aware of a Personal Data Breach, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals.

The Data Protection Officer will submit the notification to the Information Commissioner on behalf of the College in line with the Information Commissioners Office guidelines.

In accordance with data protection laws, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of affected individuals, the College must communicate the Personal Data Breach to the data subject without undue delay. The communication will contain:

- In plain language, a description of the nature of the Personal Data Breach.
- Name and contact details of the Data Protection Officer or other contact point where more information may be obtained.
- A description of the likely consequences of the Personal Data Breach.
- A description of the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects.

Data Protection Impact Assessments should be reviewed following a Personal Data Breach, or carried out where not yet in place.