Myerscough College
Opportunities for all to succeed

Data Protection Policy and Procedure

Myerscough College and University Centre is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The new regulatory environment demands higher transparency and accountability in how we as a College manage personal data. It also gives new and stronger rights for individuals to understand and control the use of their personal data.

As an organisation that collects, uses and stores personal data about its prospective applicants, students and their parents/guardians, employees, governors and commercial customers, the College recognises that having effective controls around all aspects of personal data is essential in order to demonstrate compliance with data protection legislation.

The purpose of this policy is to ensure that all College staff are fully aware of their responsibilities in terms of what they must do to ensure the correct and lawful processing of personal data.

This policy applies to all staff (including temporary and agency workers, contractors and volunteers) and Governors across all centres of the College. Any breach of this policy or of the Regulation itself will be considered an offence and the College's disciplinary procedures may be invoked. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the College.

1. Six Principles of GDPR

Myerscough College and University Centre will comply with the following six principles when processing personal data, ensuring at all times that it is:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and, where necessary, kept up to date.
5. Retained for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Myerscough College and University staff and others who process or use any personal data must ensure that they follow these principles at all times.

2. Lawful Basis for Processing Personal Data

Before any processing activity takes please, the College will establish the appropriate lawful basis for such processing, which must be one of the following:

- that explicit consent has been received from the data subject;
- that the processing is necessary for the performance of a contract to which the data subject is involved (or prior to entering into a contract);
- that the processing is necessary for compliance with a legal obligation to which the College is subject;
- that the processing is necessary for the protection of the vital interests of the data subject;
- that the processing is necessary for the performance of a task carried out in the public interest;
- that the processing is necessary for the purposes of the legitimate interests of the College or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

Except where the processing is based on consent, the College will take steps to satisfy itself that that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose). We will then document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.

We will include information about both the purposes of the processing and the lawful basis for it in the relevant Privacy Notices, and, where sensitive personal data is processed, will identify and document the lawful special condition for the processing of this data.

To meet its obligations under GDPR and the Data Protection Act 2018, Myerscough College and University Centre will:

- Ensure any new or planned projects that involve Personal Data are preceded with a Data Privacy Impact Assessment.
- Ensure that access controls are limited to role relevance.
- Ensure that any personal data is collected in a fair and lawful way.
- Obtain and record explicit consent where required.
- Explain at the outset why information is being collected, what it will be used for and with whom it will be shared.
- Ensure that only the minimum amount of information needed is collected and used.
- Ensure the information used is up to date and accurate.
- Review the length of time information is held, in line with JISC recommendations and other relevant legislation.
- Ensure information is kept securely.
- Ensure the rights that individuals have in relation to their personal data can be exercised.
- Dispose of personal data securely and without unnecessary delay.
- Ensure that anyone managing and handling personal data is competently trained to do so.
- Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do.
- Ensure that any disclosure of personal data is in line with relevant legislation, and internal policies and procedures.
- Ensure that any sharing of data to third parties is covered by a data sharing agreement.

3. Definitions

Personal Data means data relating to a living individual who can be identified from that data (or from that data together with other information that we hold). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Sensitive Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data Controllers are the organisations who determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. Myerscough College and University Centre is the Data Controller of all personal data collected and used in our business for our own purposes.

Data Users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this Data Protection Policy and any applicable data security procedures at all times.

Data Processors include any organisation that processes personal data on our behalf and on our instructions. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Myerscough College and University Centre is a Data Processor for the personal data we are obliged to process on behalf of Data Controllers such as the Education & Skills Funding Agency (ESFA), the Office for Students, managing agents for apprenticeships/services and others.

4. Data Privacy Impact Assessments (DPIAs)

New data protection legislation has introduced a new requirement to carry out a risk assessment in relation to the use of personal data for a new service, product or process. This must be done prior to the processing by means of a Data Protection Impact Assessment (DPIA). A DPIA should be started as early as practical in the design of processing operations. The process is designed to identify:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal data.

5. Privacy Notices

The College will produce and publish Privacy Notices, informing individuals from whom we collect information about the personal data that we collect and hold relating to them, how they can expect their personal data to be used and for what purposes. We will take appropriate measures to provide information by means of Privacy Notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6. Data Protection Officer

Under GDPR legislation, it is mandatory that Myerscough College and University Centre appoints a Data Protection Officer whose role will be to:

- provide information and guidance on the processing of all personal data;
- monitor the College's compliance with GDPR and highlight key risk areas to senior management;
- design and deliver relevant GDPR training activities and promote a culture of compliance;
- develop, implement and enforce an appropriate and relevant Data Protection Policy and ensure it is reviewed on a regular basis;
- establish and maintain a register of data owners for each set of information and ensure data owners understand their responsibilities; assist with investigations into notifications about breaches and maintain a log of incidents and remedial recommendations and actions;
- advise on the necessity of Data Protection Impact Assessments, the manner of their implementation and outcomes; act as the organisational contact to the Information Commissioner's Office for all data protection issues, including breach reporting; act as the contact for data subjects on privacy matters, including compliance with Subject Access Requests.

7. Staff Responsibilities

All new staff will be required to complete mandatory data protection training as part of their induction and existing staff will be required to undertake initial mandatory training as well as refresher training on a regular basis.

Employees of Myerscough College and University Centre are expected to:

- Familiarise themselves and comply with the six data protection principles.
- Ensure their own personal information is accurate and up to date.
- Keep personal data for no longer than is necessary in line with retention guidelines and relevant legislation (Data Retention Policy).
- Ensure that any personal data they process is secure and in compliance with IT Policies and Procedures.
- Acknowledge the rights of data subjects (right of access to all their personal data held by Myerscough College and University Centre) and comply with access to those records.

- Ensure personal data is only used for the purposes specified and is not unlawfully used for any other business.
- Obtain the appropriate consent, where necessary, when collecting, sharing or disclosing personal data.

All members of staff are responsible for ensuring that any personal data that Myerscough College and University Centre holds, and for which they are responsible, is kept securely and is not under any circumstances disclosed to any third party unless that third party has been specifically authorised by the College to receive that information and has entered into a confidentiality or data sharing agreement.

All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with the Information Security and Acceptable Use Policies.

Care must be taken to ensure that PC monitors and screens on other devices are not visible, except to authorised staff of the College.

Manual records containing personal data must not be left where they can be accessed by unauthorised personnel and may not be removed from College premises without explicit authorisation.

Personal data must only be deleted or disposed of in line with the Data Retention Policy.

Manual records that have reached their retention date are to be disposed of as 'confidential waste'.

Members of staff are responsible for keeping their own personal data up to date. Staff must let the College know if the information they have provided to the College changes (for example if they move house or change the bank or building society account to which they are paid).

Members of staff may have access to the personal data of other members of staff, students and other clients and suppliers of the College in the course of their employment or engagement. If so, the College expects such members of staff to help meet the College's data protection obligations to those individuals.

Members of staff must:

- Only access the personal data that they have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation to do so;
- Keep personal data secure by complying with policies on computer access, password protection and secure file storage and destruction.

- Not remove personal data, or devices containing personal data (or which can be used to access it), from the College's premises unless appropriate security measures are in place (such as encryption or password protection) to secure the information and the device.
- Not store personal data on local drives or on personal devices that are used for work purposes.
- The College's Data Protection Officer should be contacted if anyone is concerned or suspects that one of the following has taken place (or is taking place or likely to take place):

    - Processing of personal data without a lawful basis or, in the case of sensitive personal data, without also one of the conditions being met to do so;
    - Access to personal data without the proper authorisation;
    - Personal data not kept or deleted securely;
    - Removal of personal data, or devices containing personal data (or which can be used to access it), from the College's premises without appropriate security measures being in place;
    - Any other breach of this policy or of any of the data protection principles set out in in this policy.

8 Data Security

The College will use appropriate technical and organisational measures in accordance with the College's Information Security Policy and related Codes of Practice to keep personal data secure from the point of collection to the point of destruction, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- Making sure that, where possible, personal data is anonymised or encrypted.
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Staff are responsible for ensuring that any personal data they hold is kept securely and not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party (e.g. papers left on desks, telephone discussions that reveal personal information in the presence of an unauthorised person). Best practice should be followed to ensure that personal data for any individual is held only on approved College systems, i.e. student records system, staff records system.

Data security will be maintained by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which they are processed.

- Availability means that authorised users should be able to access the data if needed for authorised purposes. Personal data should therefore be stored on the College's computer system instead of individual workstations.

Security procedures include:

- Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold personal information of any kind.
- Methods of disposal - paper documents should be disposed of using the confidential waste disposal system.
- Digital storage devices - should be physically destroyed when they are no longer required.
- Equipment - staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from or otherwise secure their workstation when it is left unattended.
- Endpoint protection - staff should ensure that portable devices (e.g. memory sticks, laptops and smartphones) employ PIN or password protection and encryption technologies.

9. Data Sharing

There are occasions when it is necessary for the College to share data with other organisations, particularly to meet contractual and legal obligations. Where the College cannot identify a lawful basis for the sharing of data, the explicit consent of the data subject will be required to share personal information for that particular purpose.

Where personal information is shared, the College will ensure that data sharing agreements are in place and that all third party organisations are able to offer assurances as to the systems and processes they have in place to ensure compliance with data protection legislation.

10. The Rights of the Data Subject

Individuals have a right under GDPR to ask Myerscough College and University Centre if it holds their personal data, and if so, be provided with a copy of it.

Any person wishing to exercise this right must apply either in writing or by email to the College's Data Protection Officer:

Data Protection Officer
Myerscough College
St Michaels Road
Bilsborrow
Preston
PR3 0RY
Email: dpo@myerscough.ac.uk

The following information will be required to confirm the identity of the data subject before the information is provided:

- Full Name
- Date of Birth
- Student Number or Staff Number

The College may also require proof of identity, in which case the following forms of ID will be acceptable:

- Birth Certificate
- Passport
- Driving Licence

The College will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within one month as required under GDPR from receiving the written request. The College will provide the information in a clear format that is easily understood and in a format suitable for the requester's needs. The College may request further details to clarify the exact requirements prior to the start of the one month.

Anyone whose personal information is processed by the College processes has the right to know what information the College holds on them and to receive this information in a clear format.

It is a criminal offence for any user to alter, illegally access, deface or remove any record (including emails) following receipt of an information request. The College will take necessary action against any individual who is found to have carried out this act, which may result in disciplinary or legal action.

11. Retention and Disposal of Data

The College will retain information about students, staff and others for as long as is reasonable and necessary to comply with the law and for legitimate business needs. For students this will include information needed in connection with administering student applications, enrolment, attendance, achievement, success, post-college destinations, tutor notes, academic records, and information required for references, and in the case of prospective students, in relation to any enquiries, applications and interviews. For staff, this will include information needed in connection with their contract of employment and administering pensions and taxation, for potential or current disputes or litigation regarding employment, in the case of job applicants, in relation to any complaints or claims regarding the selection process, and information required for job references.

The College will dispose of data in line with the College's Data Retention Policy, written in conjunction with JISC recommended data retention principles and any legal and funding audit requirements. Once the retention period has elapsed, the College will ensure that any information is destroyed by secure means, ie by confidential disposal of hard copy documents and deletion/anonymisation of electronic/digital data. The College will use a reputable ISO Accredited company and obtain destruction certification.

12. Data Breaches

If anyone believes personal data held by the College has been compromised in some way they must report this immediately by notifying the Data Protection Officer: dpo@myerscough.ac.uk.

Certain breaches must be reported to the Information Commissioner's Office (ICO) and the Data Protection Officer will undertake an assessment of the likelihood and severity of any risk to people's rights and freedoms following the breach. Where this is found to be the case, we are required to notify the ICO within 72 hours of discovering that the breach has taken place and the DPO will be the nominated person to contact the ICO.

The ICO has the power to issue a monetary penalty for an infringement of the provisions of GDPR and there are two tiers of penalty for an infringement - the higher maximum and the standard maximum. The higher maximum amount is 20 million Euros (or equivalent in sterling) or 4% of the total annual turnover in the preceding financial year, whichever is higher. The standard maximum amount is 10 million Euros (or equivalent in sterling) or 2% of the total annual turnover in the preceding financial year, whichever is higher.

A personal data breach is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss, destruction, alteration or unauthorised disclosure of personal data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of an action by a member of staff.

There are three main types of Personal Data breach, which are as follows:

Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a member of staff is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people "blagging" access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong recipient, or disclosing information over the phone to the wrong person;

Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key; and

Integrity breach - where there is an unauthorised or accidental alteration of personal data.

The College takes the risk to security loss very seriously and adheres to the legal framework set down by the Information Commissioner's Office and industry standards. The College has a Breach Management Procedure to be followed in the event of a data breach or suspected data breach to ensure the College responds and manages effectively any breach in line with GDPR recommendations.

Actions may include:

- Containment and recovery – the College will respond to the incident immediately, which includes a recovery plan and, where necessary, implement procedures for damage limitation.
- Assessing the risks – the College will assess any risks associated with a breach, as these could affect any procedures after the breach has been contained. In particular, the College will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to re-occur.
- Notification of breaches – if appropriate the College will inform a data subject about an information security breach, the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.
- Evaluation and response – the College will investigate the cause of the breach and evaluate the effectiveness of any response made. If necessary, the College will update its policies and procedures accordingly.

Documents Associated with this Policy

Data Retention Policy and Procedure
Information Security Policy and Procedure
Information Security Incident and Data Breach Policy and Procedure
Staff Acceptable Use Policies and Procedures

Document History			
Author:	Director of Corporate Services	**Ref and Document Version:**	Data Protection Policy and Procedure – V2
Approval:	Senior Leadership Team	**Approval Date:**	October 2018, Updated June 2019
Review Date:	October 2021		
Publication:	Staff Intranet College Website		

Quality Assurance	
This Policy and Procedure maps to the following external quality assurance frameworks	
Framework	**Framework Section Reference(s)**
Education Inspection Framework	
MATRIX	
QAA	
QIA	
ESFA	

Key Changes to the Document
12. Data Breaches: • Where the rights and freedoms of individuals are infringed by the loss of personal data, such instances must be reported to the ICO within 72 hours. • Fines that may be imposed by the ICO for such a data breach can vary between 10 million Euros or 2% of annual turnover and 20 million Euros or 4% of annual turnover, dependent upon the infringement.

All Myerscough College Policies are subject to screening for Equality Impact Assessment

Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, marriage or civil partnership, sex or sexual orientation.

Myerscough College not only fulfils its legal position in relation to current and future equality legislation, but additionally goes beyond compliance in providing and promoting "Opportunities for all to succeed", free from any aspect of discrimination, harassment or victimisation.

All staff, Governors and volunteers have a duty of care to look after the interests of and support their colleagues. *This policy takes account of* our commitment to eliminating discrimination, identifying and removing barriers and providing equal opportunities for our learners, staff and visitors to ensure that no one feels excluded or disadvantaged.

Safeguarding, Child Protection, Prevent and Missing from Education

All staff, Governors and Volunteers have a responsibility to support and promote the College's commitment to providing a safe environment for students, staff and visitors. Additionally, all staff have a responsibility to report any safeguarding or Prevent issues to the Designated Senior Lead for Safeguarding and Prevent.