MAYFLOWER
COLLEGE

GDPR POLICY
(General Data Protection Regulation)

GDPR POLICY
Table of contents

1. GDPR POLICY STATEMENT ..... page 3
2. PURPOSE AND SCOPE OF THE POLICY 3
3. DEFINITION OF GDPR (DATA PROTECTION) TERMS 4
4. GDPR PRINCIPLES 5
5. GDPR RIGHTS FOR INDIVIDUALS 6
6. OBTAINED & PROCESSED FAIRLY 6
7. THE LAWFUL BASIS FOR PROCESSING DATA 7
8. CONSENT 8
9. SPECIAL CATEGORY DATA 8
10. CRIMINAL OFFENCE DATA 8
11. USED & DISCLOSED ONLY IN WAYS COMPATIBLE WITH PURPOSE 9
12. KEPT SAFE & SECURE 9
13. ACCURATE & COMPLETE DATA 9
14. TIMELY PROCESSING 10
15. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS 10
16. DEALING WITH SUBJECT ACCESS REQUESTS 10
17. PROVIDING INFORMATION OVER THE TELEPHONE 10
18. REVIEW OF POLICY 10

1. GDPR POLICY STATEMENT

Everyone has rights with regard to how their personal information is handled. During the course of the Mayflower College's activities the Mayflower College may collect, store and process personal information about staff, homestay accommodation providers, suppliers, students and customers, and the Mayflower College recognises the need to treat this data in an appropriate and lawful manner. The Mayflower College is committed to complying with its obligations in this regard in respect of all personal data it handles.

The types of data information that the Mayflower College may be required to obtain include details of current, past and prospective employees, suppliers, customers, students, test candidates and others that the Mayflower College communicates with. The information, which may be held on paper or on a computer or other media, as well as hard copies is subject to certain legal safeguards specified in the The Data Protection Act 1998 ('the Acts') and other regulations. The Acts impose restrictions on how the Mayflower College may collect and process that data.

The GDPR (General Data Protection Regulation) is Europe's new framework for data protection laws. It replaces the previous data protection directive, which current UK law is based upon. The new regulation started on 25 May 2018 and will be enforced by the Information Commissioner's Office (ICO). This legislation extends the current UK law by requiring that Mayflower College:

- Informs individuals why information is collected (and when);
- Ensures personal data is processed lawfully, fairly and in a transparent manner in relation to individuals;
- Informs individuals when their information is shared, why and with whom;
- Checks the quality and accuracy of information stored;
- Ensures information is not retained for longer than necessary;
- Ensures that when obsolete information is destroyed it is done so appropriately and securely;
- Ensures safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Shares information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information (known as Subject Access Requests);
- Ensures staff are aware of (and understand) policies and procedures.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

2. PURPOSE AND SCOPE OF THE POLICY

This policy sets out the Mayflower College rules on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information.

If an employee considers that the policy has not been followed in respect of personal data about themselves or others they should raise the matter with their manager as soon as

possible.

3. DEFINITION OF GDPR (DATA PROTECTION) TERMS

Personal data
The GDPR applies to 'personal data' meaning any information relating to an identifiable person. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. Data subjects for the purpose of this policy include all living individuals about whom the Mayflower College holds personal data

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information that is in, or is likely to come into, the possession of the data controller). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Sensitive personal data
The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems. This includes IT systems and CCTV systems.

The GDPR applies to 'controllers' and 'processors'.
A controller determines the purposes and means of processing personal data.
At Mayflower College this is the Director, General Manager and Director of Studies. Data controllers are people who decide what data is collected, what it is used for, and how it is stored;

A processor is responsible for processing personal data on behalf of a controller, i.e. the staff of Mayflower College.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with

processors comply with the GDPR.
The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Data processors include employees whose work involves using personal data. Data processors have a duty to protect the information they handle by following the Mayflower College's data protection and security policies at all times.

Processing means performing any operation or set of operations on data, including:
obtaining, recording or keeping data,
collecting, organising, storing, altering or adapting the data,
retrieving, consulting or using the data,
disclosing the information or data by transmitting, disseminating or otherwise making it available,
aligning, combining, blocking, erasing or destroying the data.

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, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. GDPR PRINCIPLES

Personal data shall be processed fairly and lawfully.
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Personal data shall be accurate and, where necessary, kept up to date.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Personal data shall be processed in accordance with the rights of data subjects under the Act.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. GDPR RIGHTS FOR INDIVIDUALS

The GDPR includes 8 rights for individuals, and these are as follows:

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; and
8. the right not to be subject to automated decision-making including profiling.

The rights an individual is entitled to depends on the lawful basis on which their data is being processed. For example, some rights will not apply when data is processed under certain legal bases. It is important that an organisation makes the legal basis for processing an individual's rights clear from the outset with its privacy notice.

6. OBTAINED & PROCESSED FAIRLY

Every organisation that offers goods and services to people in the EU or collects and analyses data tied to EU subjects needs to be compliant to GDPR, including organisations based outside of Europe.

The GDPR applies to 'controllers' and 'processors'.

Controller: the data controller is the person or organisation who collects data and decides what purpose that data is used for and by whom. The controller shall be accountable for, and be able to demonstrate compliance. The controller must set appropriate measures to ensure data processing is performed in accordance with GDPR, such as developing an organisational data protection policy and allocating responsibilities for data protection. If a processor is used to carry out data processing on behalf of a controller, the controller shall ensure the processor can provide sufficient guarantees that the processing will meet GDPR requirements.

Joint Controllers at Mayflower College are the Director, General Manager and Director of Studies. (Joint Controllers: when more than one controller is involved in deciding the purpose and means of processing).

Processor: the processor is a person or organisation who processes the data as instructed by

or on behalf of the controller.

The Processors at Mayflower College include Mayflower College staff and stakeholders.

Both the controller and the processor can be held legally responsible for a data breach. The Acts are intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Mayflower College), the purpose for which the data is to be processed by the Mayflower College, and the identities of anyone to whom the data may be disclosed or transferred.

7. THE LAWFUL BASIS FOR PROCESSING DATA

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Acts. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. Any employee personal data collected by the Mayflower College is used for ordinary Human Resources purposes. Where there is a need to collect employee data for another purpose, the Mayflower College will notify the employee of this and where it is appropriate will get employee consent to such processing.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Sometimes more than one legal basis may apply and the data subject should always be

informed.

Please see appendix 1.0 for information on processing data at Mayflower College..

8. CONSENT

Consent is one of the legal bases for processing personal data. GDPR states that 'consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her'. In practice, this means that consent must be given by an opt-in action by the individual; pre-ticked boxes, silence and inactivity do not constitute consent.

Consent requests should be separate from other terms and conditions, and clearly cover the purpose and the types of processing activity. Should the organisation wish to use the data for any other purposes outside of the consented purpose, then a new consent should be sought from the data subject. A consent request should cover the following information:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

Consent cannot be freely given when there is a clear imbalance between the data subject and the controller i.e. between school and pupil, prison and inmates, employer and employee. For this reason, public authorities, employers and organisations such as schools would normally rely on one of the other legal basis for processing.

9. SPECIAL CATEGORY DATA

Special category data is personal data which GDPR classifies as more sensitive, so requires additional protection.

- Race and ethnic origin;
- Political alignment and religion;
- Trade union membership;
- Genetics and biometric information;
- Health, sex life or sexual orientation.

This data may only be processed if certain conditions are met, for example you have been given explicit consent for the processing of this data or processing is necessary to protect the vital interest of the individual.

10. CRIMINAL OFFENCE DATA

An organisation may only process personal criminal offence data if the organisation is processing the data in an official capacity or has specific legal authorisation to do so. A comprehensive criminal record may only be kept under the control of an official authority.

Personal Data of children (under 18's)

GDPR states that children merit special protection under GDPR, especially when their

personal data is used for the purposes of marketing or creating personality or user profiles. You should take into account the child's level of understanding and provide an age-appropriate privacy notice. Generally speaking, the same principles, rights and legal basis apply to processing children's personal data, however if you are providing social networking services to children under the age of 16, you must obtain consent from the child's parent or guardian.

11. USED & DISCLOSED ONLY IN WAYS COMPATIBLE WITH PURPOSE

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

12. KEPT SAFE & SECURE

The Mayflower College and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Acts require the Mayflower College to put in place procedures and technologies to maintain the security of all personal data. Personal data may only be transferred to a third-party data processor if the third party has agreed to comply with those procedures and policies or has adequate security measures in place.

The following must be maintained to ensure the following:
(a) Confidentiality - that only people who are authorised to use the data can access it. The Mayflower College will ensure that only authorised persons have access to an employee's personnel file and any other personal or sensitive data held by the Mayflower College. Employees are required to maintain the confidentiality of any data to which they have access.
(b) Integrity - that the personal data is accurate and suitable for the purpose for which it is processed.
(c) Availability - that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:
(a) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
(b) Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs or any other data storage systems should be physically destroyed when they are no longer required.
(c) Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. ACCURATE & COMPLETE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed. Employees should ensure that they notify their manager of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to data would include a change of address.

14. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. For guidance in relation to particular data retention employees should contact their manager. The Mayflower College has various legal obligations to keep certain employee data for a specified period of time. In addition, the Mayflower College may need to retain personnel data for a period of time in order to protect its legitimate interests.

15. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:
(a) Request access to any data held about them by a data controller.
(b) Prevent the processing of their data for direct-marketing purposes.
(c) Ask to have inaccurate data amended.
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

16. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for data information that the Mayflower College holds about them must be made in writing. Any employee who receives a written request in respect of data held by the Mayflower College should forward it to their manager immediately. Data subjects should be provided with their data in accordance with any such request within 40 days of receiving the request.

17. PROVIDING INFORMATION OVER THE TELEPHONE

Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the Mayflower College over the phone. In particular the employee should:
Ask the caller put their request in writing.
Refer the request to their manager for assistance in difficult situations. No employee should feel forced into disclosing personal information.

18. REVIEW OF POLICY

The Mayflower College will continue to review the effectiveness of this policy to ensure it is

achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in the law and organisational or security changes.

As the Mayflower College operates internationally and has third party service providers outside of the United Kingdom, it may be necessary in the course of business that the Mayflower College has to transfer an employee's personnel data to countries outside the European Economic Area, which do not have comparable data protection laws to the United Kingdom. The transfer of such data is necessary for the management and administration of the contracts of employment and to facilitate Human Resources administration. When this is required, the Mayflower College will take steps to ensure that the data has the same level of protection as it does inside of the United Kingdom.

Reviewed 01/12/22