MARLBOROUGH COLLEGE

DATA PROTECTION POLICY

Contents:

DATA PROTECTION POLICY

Marlborough College (the College) is registered with the Information Commissioner's Office as a Data Controller.

1. General Statement of the College's Duties and Scope

The College is required to process relevant personal data regarding members of staff, applicants, parents, volunteers, pupils, alumni and families and shall take all reasonable steps to do so in accordance with this policy. The College does not buy or sell personal data.

2. Definitions

- "The College" is Marlborough College, incorporated by Royal Charter. It includes Marlborough College Enterprise Limited and additionally covers subsidiaries and affiliated bodies including clubs and societies.
- "Pupils" is all persons studying at the college.
- "All Staff" is all staff or employees of the College, including those on temporary or part time contracts and volunteers.
- "Parental consent", includes the consent of a guardian or custodian.
- "Data Subject", is a living natural individual who is the subject of the personal data.

3. Accessibility of this document.

This policy is written using clear and plain language and is considered as age appropriate (Age 13 and above) for the accessibility of all data subjects of the College.

4. Data Protection Controller and Data Protection Officer

The College has appointed the Master, Mrs. Moelwyn-Hughes as the Data Protection Controller (DPC), and Mark Armitage as Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of current Data Protection Legislation, currently the Data Protection Act 2018 and (EU) General Data Protection Regulation 2016/679 (GDPR). The Protection of Freedoms Act 2012 is also relevant to parts of this policy.

The College is exempt from requests made under the Freedom of Information Act 2000.

5. The Principles

The College shall comply with the Data Protection principles contained in the legislation to ensure all data is:-

- Fairly and lawfully processed in a transparent manner.
- Processed for a legitimate purpose.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept for longer than necessary.
- Processed in accordance with the data subject's rights.
- Processed securely.

6. Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary or a pupils' attendance record and exam results. Personal data may also include sensitive personal data as defined in the legislation.

7. Data Security

The College will take appropriate technical and organisational steps to ensure the security of personal data.

All staff will be made aware of this policy and their duties under the legislation.

The College and therefore all staff and pupils are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to all personal data. Violations of this policy by staff may be treated as misconduct or gross misconduct.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and should be encrypted when transported offsite. Some other personal data however may be appropriate for publication or limited publication within the College, therefore having a lower requirement for data security, for example sports team lists and results, or allergy information.

Reference should also be made to *Information, Communication and Technology (ICT) Policy*, which provides more specific information on digital data protection, and best practice guides that are published and updated on Firefly https://firefly.marlboroughcollege.org/data-protection-gdpr.

8. Rights of the Data Subject

GDPR expands the rights of the data subject over previous legislation, specifically data subjects have:

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.

This policy and the published Privacy Statement are part of these rights. If you wish to exercise any of these rights, with the exception of the right to access, please contact the College department processing that information in the first case. Information on the right of access and how to exercise that are specifically detailed in this policy.

Not all rights are applicable to all personal data, and may depend on the lawful basis that personal data is being processed under.

9. Processing of Personal Data

The College maintains a Privacy Statement which details personal information processed and the legal basis for processing that data. The current version can be viewed at http://www.marlboroughcollege.org/privacy .

The College processes some personal data for purposes considered direct marketing and fund-raising. Data subjects have the right to withdraw consent to these activities.

10. Sensitive Personal Data

The College may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating medical information, gender, religion, race, sexual orientation, trade union membership, biometric and genetic information.

11. Criminal Convictions and Offences.

The College does not maintain registers of or process data on Criminal Convictions and offences, other than is required for safeguarding purposes. Specifically, Enhanced DBS checks are required for all staff and unsupervised contractors. Where convictions or adverse findings are present that data is used as part of a risk assessment.

12. Rights of Access to Information (Subject Access Request or 'SAR')

Data subjects have the right of access their Personal data held by the College, subject to the provisions of current Data Protection legislation. Any data subject wishing to access their personal data should put their request in writing to the DPC or DPO. The College will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within one month for access to personal data and 21 days to provide a reply to a Subject Access Request. The information will be made available to the data subject as soon as is reasonably possible after it has come to the College's attention and in compliance with the relevant legislation. Proof of identity is required before any information will be made available.

Only the DPC or DPO may accept or respond to a Subject Access Request. Any other staff receiving such a request MUST immediately pass it to the DPC / DPO for processing or refer the person making the request to the DPC / DPO.

13. Exemptions

Certain personal data or obligations are exempted from the some of the provisions of the Data Protection legislation which includes matters such as processing for National Security and Public Security, the prevention or detection and prosecution of criminal offences. The above are examples only of some of the some of the exemptions under the legislation. Any further information on exemptions should be sought from the DPC or DPO.

14. Accuracy

The College will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the College of any changes to information held about them.

15. Enforcement

If an individual believes that the College has not complied with this policy or acted otherwise than in accordance with data protection legislation, the member of staff should utilise the College grievance procedure and should also notify the DPC or DPO.

16. External Processors and Controllers

The College must ensure that data processed by external processors, for example, service providers and Cloud services including storage, web sites are compliant with this policy and the relevant legislation. All external processors and controllers must be listed in the data processing register maintained by the DPO.

17. Secure Destruction

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

18. Retention of Data

The College may retain data for differing periods of time for different purposes as required by statute or best practice, individual departments incorporate these retention times into the processes and manuals. Statutory obligations, legal processes and enquiries may also direct the retention of certain data.

The College may store some data such as registers, photographs, exam results, achievements, books and works indefinitely in its archive.

19. CCTV

The College owns and operates a CCTV network for the purposes of crime prevention & detection, and Safeguarding.
ANPR Cameras are operated for automated vehicle access.
Where a data subject can be identified, Images must be processed as personal data.

Contacts and Representatives.

The DPC and DPO can be contacted in writing via the published main college address.
The DPO can be contact via email at DPO@marlboroughcollege.org.

Author: The Bursar
Date: Summer Term 2019
Review: Lent Term 2020