



MARLBOROUGH COLLEGE

Data Protection Policy

Michaelmas Term 2023



MARLBOROUGH COLLEGE

Data Protection Policy

Contents

1.	General Statement of the College’s Duties and Scope	3
2.	Data Protection Controller and Data Protection Office	3
3.	The Principles	4
4.	Data Security	4
5.	Rights of the Data Subject	5
6.	Processing of Personal Data	5
7.	Sensitive Personal Data.....	5
8.	Criminal Convictions and Offences	5
9.	Rights of Access to Information (Subject Access Request or “SAR”)	6
10.	Exemptions	6
11.	Accuracy	6
12.	Enforcement	6
13.	External Processors and Controllers	6
14.	Secure Destruction	6
15.	Retention of Data	7
16.	CCTV	7
17.	Contacts and Representatives	7
18.	Version control.....	7

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

- 1.1 Marlborough College (the College) is registered with the Information Commissioner's Office as a Data Controller (Registered No Z5866122).
- 1.2 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 and applicable legislation. The College does not buy or sell personal data.
- 1.3 Definitions
 - 1.3.1 "The College" is Marlborough College, incorporated by Royal Charter. It includes Marlborough College Enterprises Limited and additionally covers subsidiaries and affiliated bodies including clubs and societies.
 - 1.3.2 "Pupils" is all persons studying at the College.
 - 1.3.3 "All Staff" is all staff or employees of the College, including those on temporary or part time contracts and volunteers.
 - 1.3.4 "GDPR" used in this document and in the College privacy notice can be interpreted as either the (EU) "General Data Protection Regulation 2016/679" (GDPR) or the "Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019" (UK GDPR).
 - 1.3.5 "Consent" in this document refers to the definition of consent in GDPR.
 - 1.3.6 "Parental consent" includes the consent of a guardian or custodian.
 - 1.3.7 "Customer" is a legal person acquiring goods or services from Marlborough College Enterprise Limited or subsidiaries and affiliated bodies including events, Summer School, School of English and Culture and retail outlets.
 - 1.3.8 "Data Subject" is a living natural individual who is the subject of the personal data.
- 1.4 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.

2. Data Protection Controller and Data Protection Office

- 2.1 The College has appointed the Bursar, Mr A G Hart, as the Data Protection Controller (DPC) who, with the support of the Data Protection (DP) Office, 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 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (UK GDPR) 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 DP Office maintains data protection records, processes and procedures.

- 2.2 The College is exempt from requests made under the Freedom of Information Act 2000.
- 2.3 The College is not required to appoint an EU representative or identify a lead supervisory authority in the EU.

3. The Principles

- 3.1. The College shall comply with the data protection principles contained in the legislation to ensure all data is: -
 - 3.1.1. Fairly and lawfully processed in a transparent manner
 - 3.1.2. Processed for a legitimate purpose
 - 3.1.3. Adequate, relevant and not excessive
 - 3.1.4. Accurate and up to date
 - 3.1.5. Not kept for longer than necessary
 - 3.1.6. Processed in accordance with the data subject's rights
 - 3.1.7. Processed securely
 - 3.1.8. Personal data
- 3.2. 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 pupil's attendance record and exam results. Personal data may also include sensitive personal data as defined in the legislation.
- 3.3. Be aware that anything you write, type, document, email etc. about someone may end up being in scope of a Subject Access Request and may end up being disclosed or in the public domain.

4. Data Security

4.
 - 4.1. The College takes appropriate technical and organisational steps to ensure the security of personal data.
 - 4.2. All staff will be made aware of this policy and their duties under the legislation.
 - 4.3. The College, and therefore all staff and pupils, is 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.
 - 4.4. 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/approved systems or services and should be encrypted when transported off site. 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.

- 4.5. Reference should also be made to the 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](#).

5. Rights of the Data Subject

- 5.1. 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
- 5.2. This policy and the published Privacy Notice 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.
- 5.3. Not all rights are applicable to all personal data and may depend on the lawful basis that personal data is being processed under.

6. Processing of Personal Data

- 6.1 The College maintains a Privacy Notice which details personal information processed and the legal basis for processing that data. The current version can be viewed [here](#). This notice is updated from time to time as necessary.
- 6.2 The College processes some personal data for purposes considered to be direct marketing and fundraising.

7. Sensitive Personal Data

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

8. Criminal Convictions and Offences

- 8.1 The College does not maintain registers of, or process, data on criminal convictions and offences, other than what 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.

9. Rights of Access to Information (Subject Access Request or “SAR”)

- 9.1 Data subjects have the right of access to 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 DP Office. 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. Relevant proof of identity is required before any information will be made available.
- 9.2 Only the DPC or DP Office may accept or respond to a subject access request. Any other staff receiving such a request **MUST** immediately pass it to the DPC/DP Office for processing or refer the person making the request to the DPC/DPO.

10. Exemptions

- 10.1 Certain personal data or obligations are exempted from 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 DP Office.

11. Accuracy

- 11.1 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.

12. Enforcement

- 12.1 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 DP Office.

13. External Processors and Controllers

- 13.1 The College ensures that data processed by external processors, for example, service providers and cloud services (SAAS) including storage, websites or web applications, etc. 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 DP Office. No member of staff is authorised to purchase or make use of ICT systems or cloud-based services that process personal data without consultation with the DP Office, appropriate data protection processes having been followed, Data Protection Impact Assessment (DPIAs) completed and approvals given by the DPC and compliant contracts being in place. If you are not sure, you are responsible for initiating a compliance discussion with the DP Office/DPC.

14. Secure Destruction

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

15. Retention of Data

- 15.1 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 their processes and manuals. Statutory obligations, legal processes and enquiries may also direct the retention of certain data.
- 15.2 The College may store some data such as registers, photographs, exam results, achievements, books and works indefinitely in its archive.

16. CCTV

- 16.1 The College owns and operates a CCTV network for the purposes of protection of assets, crime prevention and detection, safeguarding and public safety. ANPR Cameras are operated for automated vehicle access. Where a data subject can be identified, CCTV images must be processed as personal data.

17. Contacts and Representatives

- 17.1 The DPC and DP Office can be contacted in writing via the published main College address.
- 17.2 The DP Office can be contact via email at DPO@marlboroughcollege.org.

18. Version control

Author:	Bursar
Approved by:	The Master
Date:	Michaelmas 2023
Review Date:	Michaelmas 2024
Circulation:	College Website, A-Z Policies, Firefly