



## Data Protection Policy

### Definitions

**College** - Brockenhurst College.

**Data Breach** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Data Controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Data Processor** - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**EEA** – European Economic Area

**ICO** – The Information Commissioner’s Office, the UK’s data protection regulator.

**Personal Data** – any information relating to an identified or identifiable natural person (**Data Subject**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Processing Data** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other making available, alignment or combination, restriction, erasure or destruction.

**Sensitive Personal Data** – data revealing ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data containing health or a person’s sex life or sexual orientation.

### Introduction

Brockenhurst College (the College) takes its responsibilities with regards to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 very seriously. The document provides the policy framework through which effective management of Data Protection matters can be achieved. The purpose of this policy is to ensure that the College and its staff comply with GDPR and the Data Protection Act 2018 when processing personal data.

Brockenhurst College is the data controller. The College holds personal data about students, parents, staff and other individuals in order to carry out its business and provide its services. For example, this information could include name, address, email address and date of birth. No matter how it is collected, recorded and used, this personal information must be dealt with properly to ensure compliance with data protection legislation.

## **Scope of the Policy**

This Policy sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles, uses, transfers and stores Personal Data. This policy applies to all staff, who should be familiar with this policy and comply with its terms. This policy applies regardless of where the data is held i.e. if the personal data is held on personally-owned equipment or outside College property. This policy also applies to any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV), and sound recordings.

This policy has been formulated in the context of the College IT Security Policy and the Data Protection Procedures.

## **The Principles of Data Protection**

Any member of staff processing personal data must comply with the six principles of GDPR. The principles require that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specific, 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.
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
- 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 appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the individuals.
- 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.

Additionally, GDPR also requires that:

- The data controller be responsible for, and be able to demonstrate, compliance with the principles.

The College is fully committed to complying with all these principles with respect to all personal data processing. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College and its staff adhere to these principles and can demonstrate compliance.

## **Responsibilities**

**The College's** responsibilities are to:

- Ensure that the College is registered with the Information Commissioner's Office.
- Establish policies and procedures and ensure that they are up to date and comply with the law.
- Ensure that staff know about and understand this policy.
- Provide staff with data protection training.

**The Compliance Officer's** responsibilities are to:

- Handle subject access / freedom of Information requests.
- Investigate data protection breaches.
- Draw up guidance on good data protection practice.
- Advise staff with data protection queries.

**Staff** responsibilities are to:

- Comply with this policy and any other supporting policies and procedures.
- Only access the personal data of others that they need to use.
- Make sure their own personal data provided to the College is accurate and up to date.
- Inform the College if any of their personal data changes.
- Inform the College if they become aware that any of the information that the College holds about them is not accurate.
- Ensure all personal data is kept securely.
- Ensure no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
- Ensure personal data is kept in accordance with the College's retention schedule.
- Promptly direct any queries regarding data protection, including subject access and freedom of information requests, to the Compliance Officer.
- Inform the Compliance Officer of any data protection breaches as soon as possible and support the Compliance Officer in resolving breaches.

**Students and Other Users'** responsibilities are to:

- Make sure that any personal data that they provide is accurate and up to date.
- Inform the College if any of their personal data changes.
- Inform the College if they become aware that any of the information that the College holds about them is not accurate.

## **Individuals' Rights**

The College is dedicated to ensuring that the rights of individuals about whom information is held can be fully exercised under the GDPR. These rights are:

- The right to be informed.
- The right to access.
- The right to rectification.

- The right to erasure (the right to be forgotten).
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights related to automated decision making including profiling.

## **Lawful Basis for Processing Data**

The College is responsible for identifying a lawful basis for processing personal data. This is stated in the College's privacy notice found on the College website.

## **Sensitive Personal Data**

Sensitive personal data or "special category data" is data that is considered more sensitive under GDPR and so needs more protection. The College is committed to ensuring that sensitive personal data in particular is kept secure and is only processed when necessary.

To ensure that sensitive personal data has greater security, the College is responsible for identifying two distinct legal bases for processing as defined under GDPR. This will also be stated as part of the College's privacy notice.

## **Subject Access Requests**

Data Subjects have a right to see all the information that the College holds on them. Should they wish to do this they should submit a request. This is known as a Subject Access Request (and could be part of a Freedom of Information Request). These should be passed to the Compliance Officer as soon as possible and the Subject Access Request (or Freedom of Information Request) Procedure should be followed.

## **Data Breaches**

In the event of a data breach, this should be reported to the Compliance Officer as soon as possible and the Data Protection Breach Procedure should be followed.

If staff are unsure whether a data breach has taken place, it should be reported to the Compliance Officer anyway, who will decide if a breach has taken place and whether the Data Protection Breach Procedure needs to be followed.

## **Retention of Data**

Personal data should only be kept for as long as is necessary to fulfil the purpose it was collected for. Once data is no longer needed, it should be disposed of securely. The College maintains a Retention Schedule detailing how long each type of record should be kept.

## **Data Processors**

There are occasions, where the personal data that we hold is processed by an external party, such as Wessex Education Shared Services (WESS) our Shared Service. Where this happens, the external party is acting as the College's Data Processor and is bound by the

College's Data Protection Policy. An agreement in writing to this effect will always be in place.

## **Data Sharing**

There are occasions where the College must share information with others, for example funding bodies, Local Authorities and Awarding Organisations/Bodies. Where this happens, the basis of the sharing is either covered in the College's contract with that organisation or is the subject of a Sharing Agreement.

Sometimes the College will share information because it is obliged to do so by law, for example, a request from the Police during their enquiries into a crime. In these situations, the College will not seek the permission from the individual concerned; neither will the College tell them that it has provided the information.

If a student or member of staff wants the College to share data with someone else, for example a solicitor or a parent/guardian, this can only be done with the student or member of staff's written consent. All such requests are dealt with under the Subject Access Request Procedure.

Sometimes the College receives requests for information under the Freedom of Information Act. The College recognises the need to balance the confidentiality of personal data against a desire to be open and transparent about its activities. However, when these two factors conflict, greater weight will always be given to data confidentiality.

## **Transferring Personal Data to a Country Outside the EEA**

GDPR impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA. So that the College can ensure it is compliant with GDPR College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

## **Further Information**

For any more information about this policy or data protection in general, please contact the Compliance Officer at [dataprotection@brock.ac.uk](mailto:dataprotection@brock.ac.uk).

More information regarding data protection can also be found on the Information Commissioner's Office website: [www.ico.org.uk](http://www.ico.org.uk).