General Data Protection Policy

Policy number:	MS181	**Policy Lead:**	VPCS
Approved by:	SLT Corporation	**Date Approved:**	23/02/2024
Review Frequency:	Annual	**Next Review Due:**	September 2024
EIA Meeting Date (if EIA required):	October 2018	**External Website Appropriate:**	Yes
SharePoint Location:	Policies and Procedures: MIS/Registers/Funding etc		
Linked Policies/College documents	• Archiving Procedure • Confidential Waste • Personal Data Breach Procedure • Privacy and Cookie Notice • Privacy Notice for Learners • Right to Access Procedure • Right to Erasure Procedure • Right to Portability Procedure • Right to Rectification Procedure • Staff Code of Conduct • Student Code of Conduct • Disciplinary Procedure		

General Data Protection Policy

1. Policy Statement and Purpose

The General Data Protection Policy of Newbury College establishes guidelines for the handling and protection of personal data, in compliance with the 2018 Data Protection Act and General Data Protection Regulation (GDPR). The policy aims to ensure personal data is treated fairly and lawfully.

Purpose

The College commits to complying with the 2018 Data Protection Act and General Data Protection Regulation (GDPR) to establish clear guidelines for the secure and lawful handling of personal data. The purpose of this policy is to establish and maintain the privacy and security of all personal data processed by the College, whether held electronically or in a physical form.

Scope

This policy applies to all staff, Corporation members, students, contractors, and any other individuals or entities that access or process personal data on behalf of the College either onsite or at a different work location.

2. Definitions

Data Subject: An individual whose personal data is being processed.

Personal Data: Information relating to an identifiable individual.

Processing: Any operation performed on personal data, whether automated or not.

3. Responsibilities

Any person who processes personal data or uses College facilities to process personal data must comply with the requirements of the General Data Protection Requirements (GDPR), the Data Protection Act 2018 and this policy.

Data Controller: Newbury College, ultimately responsible for data protection.

Information Commissioner Registration No: Z6979501

Monks Lane
Newbury
Berkshire
RG14 7TD

Data Protection Officer: Vice Principal Central Services, to monitor internal compliance, inform and advise on data protection obligations.

Designated Data Controller: The MIS Manager, who makes decisions about processing activities and handling operational data protection matters.

Staff: All people working for or with the College are responsible for the security and accuracy of their data and must ensure compliance with data processing guidelines.

Students: Students are responsible for ensuring that any information they provide to the College is accurate and current, and for informing the College of any changes to the information they have provided.

Data Protection Principles: to be followed by all: Data must be:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

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.

4. Procedures

All staff, students, contractors, and any other individuals or entities that process personal data on behalf of the College will be made aware of their data protection responsibilities.

Regular training on GDPR and data protection will be provided.

Personal data shall be processed lawfully, fairly, and transparently.

Data collection will be relevant and limited to what is necessary.

Data will be accurate and kept up to date.

Data will be retained for no longer than necessary.

Data storage will be secure, whether in paper or electronic format.

Disclosure of data will be controlled and compliant with GDPR.

Data subject access rights, including access, rectification, and erasure, will be upheld.

Appropriate technical and organisational measures will be implemented to ensure data security.

5. Compliance and Enforcement

Compliance with this policy will be monitored by the Data Protection Officer, and non-compliance may result in disciplinary action, up to and including termination of employment, enrolment or contract.

6. External References

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018

7. Supporting Documents

- Appendix A: Procedure for Responding to Data Requests.

8. Review and Monitoring

This policy will be reviewed annually to ensure its effectiveness and compliance with relevant legislation.

Reviewed: 21 December 2023, March 2024

Next review date due: September 2024

Appendix A: Procedure for Responding to Data Requests

This procedure outlines the steps for responding to requests for data held by the College, ensuring compliance with the GDPR General Data Protection Policy and other relevant legislation.

Receiving the Request:

- Requests for data, including Subject Access Requests (SARs) under the GDPR, can be received in various forms (email, letter, verbally). Staff must recognise and record the date of receipt and pass to the information services team.

Verifying Identity:

- Verify the identity of the individual making the request to ensure data is only shared with authorised persons. If identity cannot be verified, seek further information.

Logging the Request:

- Log the request in the Data Request Register, maintaining a record of the requester's details, the nature of the request, and the date received.

Assigning Responsibility:

- The Designated Data Controller will assign the request to an appropriate staff member or department, based on the nature of the data requested.

Gathering Information:

- Collect the requested data, ensuring it aligns with the request specifics. This may involve liaising with multiple departments.

Reviewing Data:

- Review the data for any sensitive information that may need to be redacted or for third-party data that cannot be shared without consent.

Compliance Check:

- Ensure the response complies with GDPR and other relevant privacy laws, particularly concerning data minimisation and purpose limitation.

Approval:

- The response, along with the data to be provided, should be reviewed and approved by the Data Protection Officer or designated authority.

Responding to the Requester:

- Respond to the requester in the same format as the request was received (e.g., written requests should receive a written response).

- Include the requested data, an explanation of any redaction or omissions, and information on their rights under GDPR (e.g., right to complain to the ICO).

Time Frame:

- Complete the entire process within the legal time frame, which is typically one month from the date of receiving the request.

Record Keeping:

- Keep a copy of the response and any correspondence in the Data Request Register for auditing purposes.

Confidentiality:

- Maintain confidentiality throughout the process. Data should only be accessed and processed by authorised personnel.

Review and Feedback:

- Regularly review and update this procedure to ensure ongoing compliance and incorporate feedback from staff and data subjects.