Newbury College

Policy number:	MS181	**Originator:**	MIS Manager
SharePoint:	Policies and Procedures: MIS/Registers/Funding etc		
EIA Meeting Date:	04 Oct 2018	**EIA Required:**	YES
Approved by:	SMT	**Date:**	21 October 2020
Review Frequency:	Annual		
Review Date:	October 2021		
External Web Site appropriate:	YES		
Linked policies/College documents:	▪ Recruitment and Selection Policy and Procedure ▪ Disclosure and Barring Service Checks Policy and Procedure ▪ Single Equality Policy and Procedure ▪ IT Code of Conduct ▪ Freedom of Information Policy and Procedure ▪ Confidentiality Policy ▪ Information Security Policy ▪ Archive and Storage Policy and Procedure ▪ Counselling Service Code of Practice		
Summary available:	This policy applies to all personal data held by Newbury College relating to staff, students and third parties. It encompasses paper records; data held on computer and associated equipment of whatever type and at whatever location, used by or on behalf of Newbury College.		

General Data Protection Policy

This document can be made available in other formats, on request

General Data Protection Policy

1.0 Background and Information

The obligations outlined in this policy statement apply to all those who have access to personal data, whether employees, Corporation members, employees of associated organisations, students or volunteers. It includes those who work at home or from home, who must follow the same procedures as they would in the College environment.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes unauthorised disclosure is liable to **disciplinary proceedings and possible prosecution**. All individuals permitted to access personal data must agree to comply with this policy.

This policy does not form part of the terms and conditions of employment for any employee of the College. However, it is a condition of employment that employees abide by the rules and policies agreed by the Corporation.

If any member of staff or student believes that the College has infringed his/her rights under this policy or is using the data to adversely affect equality and diversity or the right and freedoms of a data subject, s/he should raise this concern under the College's Grievance or Complaints Procedure respectively.

2.0 Statement of Intent

Newbury College will comply with:

- The terms of the 2003 Data Protection Act, General Data Protection Regulation (GDPR), which comes into force from 25 May 2018 and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

Further details can be accessed from:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

3.0 Confidentiality and Security

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in the General Data Protection Regulation and Data Protection Act 2003.

Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access. Duplicate records will only be made/kept on justifiable grounds, e.g. to safeguard the information against accidental loss through fire.

Computer systems will be selected/designed and computer files created with adequate security levels to preserve confidentiality. Those who use Newbury College's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work. Regular back-ups will be taken to protect against technological failure.

Personal data will be disclosed only to the data subject and other organisations and persons who are pre-defined as notified recipients. All approved recipients including third parties must sign a declaration (Appendix B / or Skillgate Declaration) to state that they understand and agree to abide by this policy. The Designated Data Controller will maintain a register of notified recipients.

Data users must comply with operating procedures specified within all related policies identified above.

4.0 Data Controller

Newbury College is the Data Controller under the General Data Protection Regulation, and the Corporation is ultimately responsible for the implementation of the Act. The Corporation has appointed the Director of Finance as the Designated Data Controller to deal with operational matters.

Information Commissioner Registration No: **Z6979501**

Data Controller: Newbury College

Monks Lane
Newbury
Berkshire
RG14 7TD

All personal data must be kept in the relevant secure central systems provided by HR, Finance, Student Services, MIS and Exams or IT Services. The Data Controller (College) must maintain a record of all data files containing personal data, whether paper or electronic media. An annual audit of secure records systems will be carried out by the Data Controller (College) in order for the required notification to the Data Protection Commissioner.

5.0 Collection of Data

Personal data of all individuals with whom we have contact (collectively referred to herein as data subjects), whether held electronically or in paper files, is covered by this policy.

Data subjects will be informed at the point at which they are expected to provide personal data of:

- the reason why the data is being collected
- to whom the information may be disclosed
- the duration for which it may be stored

This will be done when students enrol and HR Services when staff are appointed

6.0 Data Protection Principles

GDPR Article 5 (2) requires Newbury College as the data controller to be responsible for, and be able to demonstrate compliance with the following data protection principles:

Data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, 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;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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; 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 the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
5. 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.

7.0 The Rights of Data Subjects

General Data Protection Regulation has enhanced the rights of data subjects and their control over their information.

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right of data portability
- Right to object
- Right to lodge a complaint with a supervisory authority

The further details regarding the above can be found in this document. Most will have a separate policy due to the complexity of how Newbury College processes various requests by the data subject.

Right to be informed

Under GDPR Newbury College has an obligation to make any collection and use of personal data as fair, concise, transparent and accessible as possible. Whenever data is collected, the data subject must be made aware of:

- the purpose for processing the data
- the legal basis for processing
- the retention period of that personal data
- who it will be disclosed/shared with

Privacy notices are available during collection of personal data. There are different notices depending on the type of activity and category the personal data falls into for example:

- Students
- Marketing
- HR for staff

Privacy notices are version controlled so should there be any changes that could affect the 'Rights and Freedoms' of an individual, Newbury College can provide the updated version to those affected.

Right to Access

Under Article 15 GPDR data subjects have the right to access their personal data.

A subject access request or more commonly known as a SAR is simply a request by an individual, or in some cases a 3rd party, for personal information whether electronic or paper.

An individual (data subject) has the right to:

- receive confirmation that their data is/has been processed
- have access to such data whether electronic or paper based
- other information such as the lawful basis for processing the data and the retention period (most of which will be detailed in the privacy policy).

Note: A fee can no longer be charged for this service.

Please see – 'Right to Access Policy' for full instructions

Right to Rectification

Under Article 16 GPDR data subjects shall have the right to have incomplete personal data completed or corrected.

An individual (data subject) has the right to have inaccurate data corrected/rectified. This also applies to having incomplete personal data completed. A request could come verbally or in writing. A request to rectify personal data does not need to mention the phrase 'request for rectification'; it applies anytime an individual challenges the data held and this will be a valid request.

Please see – 'Right to Rectification Policy' for full instructions

Right to Erasure

Under Article 17 GPDR data subjects have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

An individual (data subject) has the right to request the deletion or removal of personal data where we have no compelling reason to storing or continued processing.

Please see – 'Right to Erasure Policy' for full instructions

Right to Restriction

Under Article 18 GPDR data subjects have the right to obtain from the controller restriction of processing.

Within the restriction are 4 sub categories; only one has to be met to allow the data subject to restrict the processing of their personal data.

i. the accuracy of the personal data is contested

ii. the processing is unlawful

iii. the College no longer needs the personal data

iv. the data subject is exercising their 'Right to Object'

Please see – 'Right to Restriction Policy' for full instructions

Right to Portability

Under Article 20 GPDR data subjects have the right to obtain and reuse their personal data for their own purposes across different services.

An individual can request a copy of their personal information in what is known as a flat file such as .csv, to enable other providers/suppliers to import the requester's data directly.

8.0 Collection of Data: Lawful, Fair and Transparent Data Processing

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in Articles 4 and 5 (GDPR).

Personal data relating to data subjects, whether held electronically or in paper files, is covered by this policy. This also includes cloud based technologies as well as many other enhancements to the regulations such as:

- mobile device
- fingerprints
- facial recognition
- retinal scans
- IP addresses

Data subjects will be informed at the point at which they are expected to provide personal data of:

- the reason why the data is being collected
- the legal basis for collection
- to whom the information may be disclosed
- the duration for which it may be stored

This will be done by all areas when students enrol and HR Services when staff are appointed.

Specific consent must be given by the data subject to the collection and processing of data classified as special category under the General Data Protection Regulation. This includes data relating to racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, or criminal offences, criminal proceedings and convictions.

Specific to students some collected details such as ethnicity and LLDD are requested for performance of a contract and to allow support.

9.0 Data Storage

Paper records containing personal data will be stored in a secure and safe manner, either in a locked filing cabinet or in a locked drawer that cannot be accessed by anyone who does not have a legitimate reason to view or process that data.

Electronic data will be password protected. Where information is required to be stored on disk, this will be kept in a locked cabinet or drawer. The computer workstations of users who regularly access and process personal data will be positioned so that they are not easily visible to casual observers and locked if left unattended. Each year IT Services, while completing their annual systems audit, will ensure that no malicious software or devices are being used at any IT terminal.

The Designated Data Controller will implement additional measures to protect the confidentiality of sensitive personal data, i.e. use of sealed envelopes within files.

This policy extends to personal data retained in archives both on and off site.

10.0 Security of Cardholder Information

Newbury College handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Newbury College commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that these commitments can be met.

Data and media containing data must always be labelled to indicate sensitivity level:

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Newbury College if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorised disclosure;
- **Public data** is information that may be freely disseminated.

All access to sensitive cardholder information should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Access to sensitive cardholder information such as the Permanent Account Numbers (PANs), personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

Media is defined as any printed or handwritten paper, received faxes, back-up tapes, computer hard drive, etc.

- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. 'Employee' refers to full-time and part-time employees, temporary employees and personnel, and consultants who are 'resident' on Newbury College sites. A 'visitor' is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- **All employees who deal with confidential data must confirm that they understand the content of this policy document by signing an acknowledgement form -** (Appendix B / or Skillgate Declaration)**.**
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the company.

Protection - All sensitive cardholder data stored and handled by Newbury College and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the company for business reasons must be discarded in a secure and irrecoverable manner.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance

Card Information is not recorded on enrolment forms or recorded on paper when payments are taken over the telephone.

11.0 Data in transit

The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises.

Information files containing personal data should not be removed from a Newbury College site without the knowledge of the Data Controller. In the event permission is granted to transport information off site, the data must be locked in a briefcase.

For transportation other than between college sites a secure courier service should be used. The status of the shipment should be monitored until it has been delivered to its new location.

12.0 Verification of Data

Responsibility falls on the data subject to ensure that any information provided to the College in connection with their studies/employment is accurate and current and that changes are notified promptly.

A regular audit will be conducted of data held on the HR Services Professional Personnel database. Staff members are expected to comply with this audit by checking and updating print outs of personal information held. Any errors identified will be rectified immediately or erased. Where this information has been disclosed to a third party, the recipient will be informed of the error.

13.0 Data Disclosure

Personal data must not be disclosed without the permission of the data subject except to users authorised to receive that data or to organisations that have a legal right to receive the data without consent being given, i.e. statutory bodies including awarding bodies, the ESFA and auditors.

A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

A parent/guardian does not have the right to see his/her child's/ward's personal record(s).

A parent/guardian may be given access to this data if the Data Controller is satisfied that either:

a. the young person has authorised the request; or

b. the request is being made in the best interests of a person who is incapable of understanding the nature of the data held, or the need for it.

Third parties claiming to have the individual's express permission to receive personal data must provide a copy of the individual's written consent on headed paper prior to data being disclosed.

Requests to confirm whether an individual attends the College as a student or is employed as a member of staff will be politely refused.

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

When requests to disclose personal data are received, it is the responsibility of the College to verify that the request is legitimate prior to issuing personal information to a third party. Staff members will be asked to provide written consent.

14.0 Data Subject Access Rights

Personal Data: Staff, students and other users of the College facilities have the right to access any personal data that the College holds about them. The request must be made in writing to the College.

Staff will be informed of their rights at induction and through publication of this policy on the internet.

Students will be advised of this right through the enrolment form. Information is also contained within the Student Handbook.

Newbury College undertakes to comply with requests for access to personal data within one month of receipt of the formal request.

If a Freedom of Information request is received, it should be referred to the DPO who should verify the identity of both parties and respond within the required timeframe.

The College can only charge if the request is deemed manifestly unfounded or excessive as endorsed by the Data Protection Commissioner.

Examination Marks and Scripts: Students are entitled to prompt access to the information about their marks for coursework and examinations. Access to examination scripts must be requested on the applicable form for each Awarding Body. The Examinations Office can provide the correct paperwork and advise on associated fees and timescales.

Please see – 'Right to Access Policy' for full instructions

15.0 Breach of Data Security

A breach of data security refers to the disclosure of personal data or information that could lead to the identification of a person. This may occur directly, such as disclosing the name, date of birth or contact details or indirectly, by supplying the IP address of a home computer.

The most common examples of breaches are:

- Access by an authorised third party, this could be as a result of a PC not locked, password sharing or hacking
- Sending personal data to an incorrect recipient or including other data subjects in the correspondence
- Not encrypting files sent externally, or even internally, if there are recipients which aren't party to the information
- Computing devices being lost or stolen – this will include phones if used to access the College network IT (even email)

- Amendment to personal data without permission or consent
- Loss or deletion of personal data
- Sensitive notes added to our MIS system not flagged as sensitive – meaning any user will be able to review
- Hacking or unauthorised network access

If a breach is identified or the data holder is uncertain if an incident constitutes as a breach, the GDPR Personal Data Breach Policy must be consulted and the incident reported to the Data Protection Officer. Should the incident involve the Data Protection Officer or member of the Senior Member Team refer directly to the 'Whistle Blowing Policy'. Any issues regarding IT such as network security must be reported to the IT Manager immediately.

Please see – 'Personal Data Breach Policy' for full instructions

16.0 Employee Responsibilities

Provision of Personal Data: All staff are responsible for ensuring that the data held by the College about them is accurate. Each member of staff must:

- ensure that any information they provide to the College in connection with their employment is accurate and current;
- inform the College in writing of any changes to the information they have provided;
- participate in the regular audit of data held on the HR Services database, updating or correcting information held on them

The College cannot be held responsible for errors in personal data if staff do not regularly update information, when changes occur, or on request.

Processing Personal Data Relating to Others on Behalf of the College: All staff must ensure that the way in which they collect, collate, store or process information on behalf of the College complies with this policy.

Staff members must inform the Data Controller of any data files containing personal data, whether paper or electronic media, that they hold in order that the Data Protection Commissioner can be notified.

17.0 Student Obligations

Provision of Personal Data: All 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.

The College cannot be held responsible for errors in personal data if students do not regularly update information, when changes occur, or on request.

Processing Personal Data Relating to Others on Behalf of the College: Any student who uses College facilities to process personal data must comply with the requirements of the General Data Protection Requirements (GDPR), the Data Protection Act 2003 and this policy.

18.0 Training

All employees who are involved in the collection and processing of personal data will be given appropriate training. This may vary as to their role, but may include some or all of the following:

- understanding the Data Protection Principles
- understanding Newbury College's policy towards Data Protection
- dealing with requests for disclosure
- procedures for data collection and processing specific to the data user

The Data Controller will be responsible for ensuring appropriate training is organised and delivered to meet this obligation (General Data Protection Regulation Training is mandatory and completed as part of CPD).

19.0 Evaluation and Monitoring

This policy and procedure will be:

- evaluated through the training and development programme for data users

And monitored in terms of:

- data audits
- adherence to the obligations as set out above
- being up to date and in line with legislation
- compliance with best practice as published on the Information Commissioner's website

The Data Controller will carry out this evaluation and monitoring and, where there are significant issues, these will be raised with the Director of Finance & Administration. A decision will be taken by both as to the right course of action.

Date: 01/05/2018
Review: Dec 2013, April 2014, Dec 2015 (minor amendments), Jan 2017 (Minor amendments), May 2018 (major GDPR amendments), Oct 2019 (no change) Oct 2020 (no change)
Next Review: October 2021