Newbury College

Policy number:	MS181	**Originator:**	MIS Manager
SharePoint:	Policies and Procedures: MIS/Registers/Funding etc		
EIA Meeting Date:	10 Feb 2017	**EIA Required:**	YES
Approved by:	CMT SMT F&GP Corporation	**Date:**	24.04.14 10.04.14 / 18.12.15 / 13.01.17 16 June 2014 30 June 2014
Review Frequency:	Annual		
Review Date:	January 2018		
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 ▪ 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.		

Data Protection Policy

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

Data Protection Policy

1.0 Background and Information

1.1 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.

1.2 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.

1.3 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.

1.4 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, 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, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful
    - Information and guidance given by the Information Commissioner's Office - https://ico.org.uk/for-organisations/guide-to-data-protection/

3.0 Confidentiality and Security

3.1 Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in the Data Protection Act 2003 (Appendix A).

3.2 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 lose through fire.

3.3 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.

3.4 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.

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

4.0 Data Controller

4.1 Newbury College as a body corporate is the Data Controller under the Data Protection Act 2003, and the Corporation is therefore ultimately responsible for the implementation of the Act. The Corporation has appointed the MIS Manager as the Designated Data Controller to deal with operational matters.

4.2 All personal data whether related to students or staff 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

5.1 Personal data related to staff, learners, or other 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.

5.2 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 by Learner Services when learners enrol and HR Services when staff are appointed

5.3 Specific consent must be given by the data subject to the collection and processing of data classified as sensitive under the Data Protection Act. 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

6.0 Data Storage

6.1 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.

6.2 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 it 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.

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

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

7.0 Security of Cardholder Information

7.1 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.

7.2 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.

7.3 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 unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7.4 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.

7.5 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.

7.6 **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.

7.7 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

7.8 All card information provided on enrolment forms or recorded from telephone contact must have all but the last 4 digits of the long card number, the issue number, start date, expiry date and security number (the 3 or 4 digit number on the signature panel on the reverse of the payment card) blacked out with a marker pen as soon as the payment has been authorised and before being stored in a locked cabinet.

7.9 **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.

7.10 The procedure for transporting documentation containing credit card details from Newbury College's Calcot Centre to Monks Lane campus is as follows:

- The documents should be secured in a sealed envelope at the Calcot Centre by the Newbury College Manager at the site
- The number of documents and identification detail is logged on the envelope
- The log book is completed at Calcot and the manager must sign out the envelope with the date, time of transportation and state the identification information on the envelope
- When the envelope arrives at Newbury College it must be signed in at reception to a designated member of the Information Services team.

7.11 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.

8.0 Data Processing

8.1 Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject.

8.2 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 brief case.

9.0 Verification of Data

9.1 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.

9.2 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.

10.0 Data Disclosure

10.1 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 SFA / EFA and auditors.

10.2 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.

10.3 **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.

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

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

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

10.7 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.

11.0 Data Subject Access Rights

11.1 **Personal Data:** Staff, learners and other users of the College facilities have the right to access any personal data that the College hold 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.

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

11.2 Newbury College undertakes to comply with requests for access to personal data within 21 days of receipt of the formal request, and in any event no longer than 40 days, the period prescribed by the Data Protection Act.

11.3 If a Freedom of Information request is received, it should be referred to MIS who should verify identity on both sides as per para 9.7 and apply College charges.

11.4 The College reserves the right to make an administrative charge for access to personal data as endorsed by the Data Protection Commissioner.

11.5 **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.

12.0 Employee Responsibilities

12.1 **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.

12.2 **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.

13.0 Learner Obligations

13.1 **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.

13.2 **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 Data Protection Act 2003 and this policy.

14.0 Training

14.1 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 (Data Protection Training is mandatory and completed as part of CPD).

15.0 Evaluation and Monitoring

15.1 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

15.2 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: 12/01/2017
Review: Dec 2013, April 2014, Dec 2015 (minor amendments), Jan 2017 (Minor amendments).
Next Review: January 2018

JS\SP\MIS\DATAPROTECTION\13.01.17