RUNSHAW COLLEGE		
POLICY TITLE: Data Protection Policy		
APPROVED BY: Remuneration and Organisational Development Committee	**AUTHOR:** Tracey Croft	
POLICY OWNER: SMT	**POSITION:** Assistant Principal - Personnel	**VERSION:** 6
LAST UP-DATED: October 2014	**REVIEW DATE:** September 2017	
IMPACT ASSESSMENT DATE: October 2011		

1 INTRODUCTION

Runshaw College keeps information about staff, students and other parties to allow it to operate as a successful Further Education institution and meet its legal obligations. To comply with the Data Protection Act 1998 ("the Act), personal data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles in the Act.

2 DATA PROTECTION PRICIPLES

In summary, the Principles state that **personal data** shall:

1. Be processed fairly and lawfully.
2. Be obtained for specified and lawful purposes, and will not be processed in a manner incompatible with those purposes.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and up to date.
5. Not be kept for longer than is necessary.
6. Be processed in accordance with the rights of the person that the data is about.
7. Be kept safe from unauthorised access, accidental loss or destruction.
8. Not be transferred to a country outside the European Economic Area, unless the country has equivalent protection for personal data.

3 PERSONAL DATA AND PROCESSING

Personal data is data relating to a living person who can be identified from that data whether stored electronically, in a paper-based filing system or in any other form or medium. Processing, for the purpose of the Act, is any operation on personal data including accessing, altering, adding to, using, disclosing, merging, deleting or destroying data.

4 DATA PROTECTION OFFICER

4.1 Runshaw College, as corporate body, is the Data Controller under the Act. Therefore Governors are ultimately responsible for monitoring this Policy and for complying with the Act.

4.2 The designated Data Protection Officer is the individual or individuals appointed by the College to carry out the day to day duties. The College has two designated Data Protection Officers: the Assistant Principal - Personnel and the MIS and Data Services Manager . They may be contacted at the Langdale Road Campus, Leyland, Lancashire. PR25 3DQ, by telephone on 01772 622677, or by e-mail (dataprotectionofficer@runshaw.ac.uk).

4.3 The Data Protection Officer will review the number and nature of requests for rights of access to data and queries raised in connection with this Policy annually and, in the light of this review, will propose any necessary changes to this Policy or related procedures.

5 REQUIREMENT TO COMPLY

5.1 Staff, students or other parties (e.g. contractors, consultants, partners) who process personal data collected in the name of the College must ensure that they follow the above Principles.

5.2 Compliance with the Act is the responsibility of all staff and students who access College systems. A breach of this Policy may lead to disciplinary action and/or access to College facilities being withdrawn, or criminal prosecution.

5.3 Questions about the interpretation or operation of this policy should be taken up with the College's designated Data Protection Officer.

5.4 Staff, students or other parties who believe that the Policy has not been followed in respect of **their own personal data** should first raise the matter with the designated Data Protection Officer. If the matter is not resolved it may be raised as a formal complaint or grievance, in accordance with College procedures.

6 NOTIFICATION OF DATA HELD AND PROCESSED

6.1 Staff, students and other persons about whom the College holds data are entitled to:

- Know what information the College holds and processes about them and why.

- Know how to gain access to it.
- Know how to update it.
- Know how the College complies with the Act.

6.2 The College will notify staff, students and other relevant parties of the nature of data that the College holds and processes about them, the reasons for which it is processed and how this can be changed.

7 RESPONSIBILITIES OF STAFF

7.1 Staff are responsible for:

- Checking the information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of changes to information they have provided.
- Checking information that the College sends to them, detailing data stored and processed about them.
- Informing the College of errors or changes in information stored. The College cannot be responsible for un-notified errors.
- Ensuring that personal data they hold about students is kept securely
- Inform the Data Protection Officer of any new uses of personal data
- Comply with the College's IT Access, Usage and E-Safety Policy
- Not disclosing any personal data which they hold on students to an unauthorised third party without consent
- Destroying personal data in accordance with College Archive and Data Retention Guidelines

7.2 If staff process information about other parties, they must comply with the guidelines for staff, detailed in Appendix 1.

7.3 Managers have a responsibility to ensure that their staff are aware of this policy receive appropriate training to enable them to comply with Data Protection Principles and adhere to retention periods to ensure that personal data is not kept for longer than is required.

8 RESPONSIBITIES OF STUDENTS

8.1 Students are responsible for:

- Checking the information that they provide to the College in connection with their enrolment/studies is accurate and up to date
- Informing the College of changes to information they have provided
- Complying with all college policies regarding the use of IT.

8.2 Students may process personal data. If they do so they must notify their teacher or tutor, who must notify the designated Data Protection Officer. A learner, teacher or tutor who requires further clarification about this should contact the designated Data Protection Officer.

9 DATA SUBJECT CONSENT

9.1 In many cases, the College can only process personal data with the consent of the individual concerned. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the College processing specified classes of personal data is a condition of acceptance of a learner onto a course and a condition of employment for staff.

9.2 The College has a legal obligation to ensure that staff are suitable for the duties and responsibilities of their role, and students for the course offered. The College also has a duty of care to all staff and students and must therefore make sure that staff and those who use College facilities do not pose a threat or danger to themselves or others.

9.3 The College also asks for certain information about the health of staff and students, which it will only use in connection with the protection of the health and safety of the individual and others, but needs consent to process.

10 PROCESSING SENSITIVE INFORMATION

10.1 It is sometimes necessary for the College to process sensitive information, such as about a person's health, criminal convictions or race. Sensitive personal data, as defined by the Act, includes information about:

- racial or ethnic origins;
- political opinions;
- religious beliefs;
- trade union membership (or non-membership);
- physical or mental health or condition;
- sex life or sexual orientation;
- criminal (or alleged criminal) activities; or
- criminal proceedings, criminal convictions (or any sentences imposed by the courts).

10.2 Sensitive personal data will be used only for the purpose it was collected such as managing the College's equality and diversity policy and related statutory obligations, recruitment, ascertaining suitability and fitness for the job or course place, managing attendance and liaison with the Young People's Learning Agency, the Skills Funding Agency or other regulatory authorities or funding providers. More information about this is available from the designated Data Protection Officer

10.3 If a person obtains a Gender Recognition Certificate while employed by or studying at the College, all records will be replaced with new details as soon as practicable. Regardless of the legal status of any individual, confidentiality regarding any previous gender identity will be maintained and any records that may be held by College which could potentially reveal a change of status will be regarded as sensitive and access restricted.

11 DATA SECURITY

11.1 Staff are responsible for ensuring that personal data that they hold on behalf of the College is (a) secure, and (b) is not disclosed to an unauthorised third party. Any member of staff that processes personal data is a Data Processor under the Act.

11.2 Unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct.

11.3 Personal information should be physically secure and, if it is computerised, it should be coded, encrypted or password protected or kept only on a medium that is stored securely.

12 RIGHTS TO ACCESS INFORMATION

12.1 Staff, students and other parties have the right to access **their** personal data that is stored by the College. Anyone who wishes to formally exercise this right must complete the "Access to information" form (Appendix 2) and give it to the designated Data Protection Officer.

12.2 For applications made by existing staff and students, the College may make a charge of up to **£10.00** on each occasion that formal access is requested, although the designated Data Protection Officer has discretion to waive this charge, having regard to the circumstances and nature of the request. For applications from other parties, the College may make an additional reasonable charge, as decided by the designated Data Protection Officer, if this is required to cover administrative costs.

12.3 The College aims to comply with requests for access to personal data within 40 calendar days of the date of receipt of the request by the designated Data Protection Officer. If for some exceptional reason this timescale cannot be met, the reason for delay will be explained in writing to the person making the request.

13 PUBLICATION OF INFORMATION

13.1 Information already in the public domain is exempt from the Act. The College makes public information available concerning its governance, annual accounts, rules, charters, significant policies and media releases, except for confidential matters and personal data, unless consent has been obtained.

13.2 Any individual who has good reason for wishing their personal data to remain confidential should contact the designated Data Protection Officer.

14 EXAMINATION RESULTS

Students are entitled to information about their results for coursework and examinations. However, this may take longer than other information to provide if third parties such as examining bodies have to be contacted.

15 RELATED POLICIES AND GUIDELINES

15.1 The College has a number of policies which are associated with the Data Protection Policy:

- IT Access, Usage and E-Safety Policy;
- Publication Scheme. The Freedom of Information Act promotes greater openness and accountability available across the public sector by requiring public authorities to make information available proactively through a Publication Scheme. The College has adopted the model further education Publication Scheme;
- DBS Policies. Safer Recruitment and Engagement Policy/Recruitment of Ex-Offenders and The Secure Handling and Use of DBS Certificates; and
- College Archive and Data Retention Guidelines.

16 MONITOR AND REVIEW

16.1 A record will be kept of all the data protection requests made of the College to and timescales to ensure that these are processed with the 40 calendar day timescale.

16.2 This policy will be reviewed at least every three years by Assistant Principal – Personnel or in line with legislative developments and the need for good practice.

APPENDIX 1

STAFF GUIDELINES FOR DATA PROTECTION

1 Most staff process data about students, e.g. when marking registers, or College work, writing reports or references, or as part of pastoral or academic supervisory roles. The College will ensure that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the Act. This information that staff deal with on a day-to-day basis will be "standard" and covers categories such as:

- General personal details e.g. name and address.
- Details about class attendance, course work marks, grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

2 Information about a student's physical or mental health, gender identity, sexual orientation, political or religious views, trade union membership, criminal record, ethnicity or race is sensitive and can only be collected and processed with the student's consent.

3 All staff have a duty to make sure they comply with the Data Protection Principles in the Data Protection Policy. In particular, staff must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Stored and disposed of securely, and in accordance with College policy.

4 Staff must not disclose personal data to any student or third party, other than the person whom the data is about, unless for normal academic or pastoral purposes, in accordance with College policy, or as required by law.

5 In situations where third parties such as contractors, consultants or partners may have access to personal data that is the responsibility of the College then the member of staff who authorises access to this data should ensure that the third party is aware of the requirements of the Data Protection Policy.

6 Staff should not disclose personal data about other staff except in accordance with College policy or if the requesting employee needs the information to perform their duties. Only College Management can provide employment references to a prospective employer, a financial reference or similar. These will be co-ordinated and centrally recorded by the Personnel Section.

7 Personal data must not be given to someone you do not know unless you can confirm the identity the person requesting the information and satisfy yourself that you can legally comply with the request. Particular care should be taken with telephone requests and alleged relatives of students and staff. Sensitive personal data must not be disclosed without the express permission of the data subject. Refer all difficult situations to the designated Data Protection Officer.

8 Police or similar legal requests for disclosure of personal data should be referred to the designated Data Protection Officer. If the officer will not wait because the

matter is urgent, the officer must issue a DP1 form. This will detail the required information and must be signed by a Superintendent. You should make a note of the officer's identification number, the information released and the date and time.

9 Personal data collected for a specified purpose should not be used for another purpose (e.g. unsolicited direct marketing).

10 Particular care should be taken with the use of E-mail or fax to transmit personal data. You will need to be certain that it has only been sent to the intended recipient. If you are the recipient, you will need to ensure that the data is retained for the appropriate length of time, remains accurate and can be retrieved when required.

11 Staff have screen-based access through the College ITfacilities to a considerable amount of personal data that is held within the central information systems. Paper-based reports are also produced from these systems. Users should ensure that only authorised persons are able to see this information.

12 Before processing personal data, consider the following checklist:

- Do you really need to record the information?
- Is the information "standard" or "sensitive"?
- If it is sensitive, has the data subject's express permission been obtained?
- Does the data subject know why this data will be processed?
- Has the data subject confirmed that the data is accurate?
- Are you authorised to collect, store, process the data?

13 When you process data, simple security measures are:

- File personal data away from sight of unauthorised persons.
- Lock personal data away and/or lock the room if it is being left empty.
- Do not leave personal data (paper based or on other media such as floppy disc, CD or pen drive) in bags or cases in situations where it may be mislaid, damaged or stolen. If possible, avoid taking such information off site.
- Seal personal data transmitted by post (internal as well as external) in envelopes or packages.
- Ensure your computer password is secure and not disclosed to anyone else.
- Log out before you leave your computer unattended.
- Position computer screens away from unauthorised view.
- Set your computer screen saver to come on after a short interval.
- Have back-ups for personal data stored on computer.
- Ensure that personal data being disposed of cannot fall into the wrong hands before it is finally destroyed. Shredding is more secure.

14 Issues concerning compliance with the Data Protection Policy should be addressed to the designated Data Protection Officer. The most frequent issues are:

(a) periods for retention of records and
(b) to notify the designated Data Protection Officer that personal data is being collected, processed and stored.

15 The designated Data Protection Officer are the Assistant Principal - Personnel and the Information Manager. They may be contacted at the Langdale Road Campus, or by e-mail.

APPENDIX 2

RUNSHAW COLLEGE

STANDARD REQUEST FORM FOR ACCESS TO PERSONAL DATA

To: The designated Data Protection Officer, Langdale Road

I wish to have access to data that the College has about me in the following categories *(ticked as appropriate)*:

1	Academic qualifications	
2	Course work marks and details	
3	Examination results (*)	
4	Academic or employment references	
5	Disciplinary records	
6	Health and medical matters	
7	Political, religious or trade union information	
8	Any statements of opinion about my abilities and performance	
9	Personal details (e.g. name, address, date of birth etc.)	
10	Other information *(specified below)*:	

(*) Provided free of charge at the time the examining body releases results, without request.

I understand that I may have to pay a fee of up to **£10.00** for the above request for access to data and my cheque for this amount, made payable to "**Runshaw College**" will be forwarded to the designated Data Protection Officer upon request and before the requested data is disclosed.

Name: *(please print, in capitals)*	
Student number or Staff I.D.:	
Signed:	
Date of request:	