RUNSHAW COLLEGE		
POLICY TITLE: Data Protection Policy		
APPROVED BY: Governors	**AUTHOR:** Alex Harding	
POLICY OWNER: Data Protection Officer	**POSITION:** IT Services Manager	**VERSION:** 9
LAST UP-DATED: November 2019	**REVIEW DATE:** November 2022	

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 EU General Data Protection Regulation ('the GDPR / Data Protection Act 2018'), 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 GDPR / Data Protection Act 2018.

2 DATA PROTECTION PRICIPLES

In summary, the Principles cover:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be 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
Integrity and confidentiality	Personal data shall be 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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR / Data Protection Act 2018

3 PERSONAL DATA AND PROCESSING

3.1 Personal data is defined as any information related 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 ID number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or social identify of that natural person.

3.2 A data processor in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.3 Processing is defined as 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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4 DATA PROTECTION OFFICER

4.1 Runshaw College is the Data Controller under the GDPR / Data Protection Act 2018 and therefore College Management are responsible for ensuring compliance with this legislation.

4.2 The designated Data Protection Officer is the individual appointed by the College to carry out the day to day duties. The College has a designated Data Protection Officer: IT Services, Print Shop & Facilities Manager who may be contacted at the Leyland Campus, Langdale Road, Leyland PR25 3DQ on 01772 642057, or by e-mail dataprotectionofficer@runshaw.ac.uk

4.3 The Data Protection Officer will review the number and nature of subject's rights requests 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.

4.4 In accordance with the requirements of GDPR / Data Protection Act 2018, the Data Protection Officer will be responsible for the reporting of any breaches that may occur to the Information Commissioners Office (ICO) within 72 hours of the College becoming aware of the breach(es).

4.5 The Data Protection Officer will act independently in relation to Data Protection issues and will make recommendations through the Data Protection Working Party, SMT Information Management and through an Annual Report to Governors.

4.6 The Data Protection Officer will:

- Inform and advise the data controller and processors who carry out processing of their obligations under GDPR / Data Protection Act 2018;

- Monitor compliance with the, policies of the controller or processor including assignments of responsibilities, awareness raising and training of staff, and input into related audits;
- Provide advice where requested as regards Data Protection Impact Assessment (DPIA) and monitor its performance;
- Co-operate with the ICO; and
- Act as the point of contact for data subjects and the ICO with regards to prior consultation or any other data protection matter as necessary

4.7 The Data Protection Officer may fulfil other tasks and duties. The College shall ensure that any such tasks and duties do no result in a conflict of interest.

5 REQUIREMENT TO COMPLY

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

5.2 Compliance with the GDPR / Data Protection Act 2018 is the responsibility of all staff, students and other parties who access College systems. A breach of this Policy may lead to disciplinary action and/or access to College facilities being withdrawn, contractual termination or criminal prosecution.

5.3 Questions about the interpretation or operation of this policy should be raised 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 update it.
- Know how the College complies with the GDPR / Data Protection Act 2018.
- Know how to exercise their individual rights under the GDPR / Data Protection Act 2018.

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. Notification will take the form of Privacy Notices, Contracts, Learning Agreements and other relevant modes of communication.

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
- Comply with the College's IT Access, Usage and Online Safety Policy
- Not disclosing any personal data which they hold on students to an unauthorised third party without consent
- Archiving and destroying personal data in accordance with the College's Archive and Data Retention Policy
- Comply with the Destruction and Disposal of Data Storage Media Procedure
- Report promptly any security concerns and/or breaches in data protection
- Inform the Data Protection Officer of proposed changes to the College's Data Register

7.2 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 other appropriate policies.

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 Where students may process personal data as part of their learning experience, teaching staff are responsible for ensuring that they comply with the College's Data Protection Policy and any other relevant procedures.

9 LAWFULNESS OF PROCESSING

9.1 Processing of personal data is legal when one or more of the following conditions is met:

- The data subject has consented.
- It is necessary to fulfil a contract between the data subject and controller.
- It is a legal requirement.
- It is necessary to protect the vital interests of the data subject or other natural person.
- It is necessary for legitimate interests pursued by the controller except where the rights of the data subject override.
- Any reuse is compatible with the original purpose of collection, or effects archiving or statistical processing.

9.2 The College will record the legal basis for processing on the College Data Register.

10 DATA SUBJECT CONSENT

10.1 To comply with the GDPR / Data Protection Act 2018, separate consent for different processing operations is required and records must be kept of the consent and the context in which it was provided.

10.2 Consent must be:

- A clear affirmative act.
- Freely given.
- Be specific and informed
- Clearly distinguishable from other matters.
- Intelligible and easily accessible.
- An unambiguous indication of the data subject's agreement (which can be be withdrawn as easily as it is given).

10.3 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. The College will take care to process personal data for legitimate reasons where this is necessary for staff to effectively manage the employment relationship or for students, to deliver their education in liaison with the Education and Skills Funding Agency (ESFA) or other regulatory authorities or funding providers.

10.4 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.

10.5 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.

10.6 Where consent is required, the College will ensure that the data subject has complete freedom in providing this consent and it will not be tied to any other form of contract or agreement.

10.7 Where the College requires consent to provide personal data to a third party this will be explicit within the request to the individual and details of the third party will be provided.

10.8 All data subjects will have the ability to withdraw or alter this consent at any time through contacting the Data Protection Officer or via contact with their College contact in each circumstance.

11 PROCESSING SPECIAL CATEGORY DATA

11.1 It is sometimes necessary for the College to process special category data, such as about a person's health or race. Sensitive personal data, as defined by the GDPR / Data Protection Act 2018, includes information about:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health;
- sex life and sexual orientation; and
- biometric or genetic data.

12 DATA SECURITY

12.1 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.

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

12.3 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.

12.4 All personal data leaving the College's secure network must be encrypted and password protected. The password must be shared with the recipient via an alternative means of communication. More information regarding encryption can be accessed by contacting the Service Desk.

13 DATA SUBJECT RIGHTS

13.1 Runshaw College have a legal obligation to affect the rights of Data Subjects under the GDPR / Data Protection Act 2018, and a number of rights are defined:

Article	Right
12	Transparency, Communication and Modalities.
13	Provision of Information regarding the Controller and Processor.
14	Provision of Information regarding data acquired from third parties.
15	Right of Access
16	Right to Rectification
17	Right to Erasure (aka Right to be Forgotten)
18	Right to Restriction of Processing
20	Right to Data Portability

13.2 Staff, students and other parties are able to exercise their rights regarding personal data that is stored by the College. Anyone who wishes to formally exercise this right should contact the Data Protection Officer and will be progressed in line with the appropriate timescales.

13.3 For the most part, applications made by existing staff and students shall be free of charge, however on occasion the designated Data Protection Officer may assess that the request is excessive, having regard to the circumstances and nature of the request. Reasonable charges may be made for requests deemed excessive. Alternatively, the Data Protection Officer may opt to refuse 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.

13.4 The College aims to comply with subject's rights requests regarding personal data without undue delay, and within 30 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 during the initial 30 day period. A further two month period may be required where a request is complex or volumes of requests prevent a prompt response.

13.5 A record will be kept of all the subjects' rights requests made of the College to and timescales to ensure that these are processed with the appropriate timescale.

14 RELATED POLICIES AND GUIDELINES

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

- IT Access, Usage and Online Safety Policy;
- Information Security Policies;
- Data Breach 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;
- Destruction and Disposal of IT Equipment and Data Storage Media Procedure.
- Archive and Retention Policy
- Staff, Student and Parent Privacy Notices
- Business Continuity Management
- Human Resources and Health and Safety Policies.

15 DATA PROTECTION IMPACT ASSESSMENTS

15.1 A Data Protection Impact Assessment (DPIA) assesses the impact of processing operations on the protection of personal data. A Single assessment may address a set of similar processing operations that present similar risks.

15.2 Where appropriate College Systems shall undergo a DPIA and consider privacy by design and default.

15.3 The Manager responsible for the process/system will carry out the DPIA and this will be reviewed and audited internally.

15.4 A DPIA will be created for any new System, Service or Process identified as handling data which is likely to result in a High Risk to individuals.

15.5 In order to classify the risk to Individuals, the ICO DPIA Screening Checklist will be completed and reviewed, where a High Risk is identified a DPIA will be completed.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

16 MONITOR AND REVIEW

16.1 This policy will be reviewed at least every three years by the Data Protection Officer or in line with legislative developments and the need for good practice.

Document Control

Document Identifier
DP Policy

Distribution List

Name	Title	School/Function
David Sharrock	Director of Facilities	Facilities
SMT- Facilities & IT		SMT
Anthony Anderson	IT Support Team Leader	IT Services
Andrew Gant	Service Desk Team Leader	IT Services
Paul Stephens	IT Systems Team Leader	IT Services
Alex Harding	Data Protection Officer	IT Services
Kevin Chadwick	Head of QMIST/DDPO	QMIST
Tracey Croft	HR Director/DDPO	HR/SMT
Data Protection Working Group		DPWG
Ryan Hough	Facilities Team Leader	Facilities
Sabrina Eckert Doyle	Facilities Team Leader	Facilities

Version History

Version	Reference	Date	Author	Comments
9.1	IM-33839	25/10/2019	Alex Harding	DPO Transfer