Riverside College
Widnes & Runcorn

# DATA PROTECTION POLICY

## 1 Introduction

1.1 The **legal basis** for this policy is compliance with the Data Protection Act 2018. The new Act writes into English law the European Union's General Data Protection Regulation (GDPR). For the purposes of this document we will refer to the Data Protection Act 2018 and any subsequent law as 'Current Data Protection Legislation'.

1.2 The College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised, and legal obligations to funding bodies and government complied with.

1.3 To comply with the law, information 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 which are set out in the Current Data Protection Legislation. In summary these principles state that personal data must be:

- processed must be lawfully, fairly and transparently.
- collected for specific, explicit and legitimate purposes, and not processed in a manner that is incompatible with the purpose for which it was collected
- adequate, relevant and not excessive in relation to the purpose for which it is processed.
- accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.
- kept for no longer than is necessary for the purpose for which it is processed.
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

1.4 The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

## 2 Status of the Policy

2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy could therefore result in disciplinary proceedings.

2.2 Any member of staff who considers that the policy has not been followed in respect of the processing of personal data should raise the matter with the Data Protection Officer.

## 3 Notification of Data Held and Processed

3.1 All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why.
- Know how to gain access to any information which is covered under the current Data Protection Legislation.
- Know how to keep it up to date.
- Know what the College is doing to comply with its obligations under the current Data Protection Legislation.

3.2 The College will therefore provide all staff and students and other relevant users with a privacy notice to comply with the requirements of the Current Data Protection Legislation.

3.3 This will include information about all the types of data the College holds and processes about them and the reason for which it is processed.

## 4 Responsibilities of Staff

4.1 All staff are responsible for processing personal data in accordance with the requirements of the Data Protection Legislation and, in particular (but without limitation) for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information which they have provided, i.e. changes of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

4.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references to other academic institutions or details of personal circumstances), they must comply with the guidelines for staff, which are set out in the document 'Data Protection Guidelines' to be found on the staff intranet.

## 5 Data Security

5.1 All staff are responsible for ensuring that:

- Any personal data, which they hold, is kept securely in accordance with Current Data Protection Legislation.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

5.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

5.3 Personal Information should be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerized or stored/accessed by electronic media,
  - be password protected; or
  - kept only on media which is kept securely.

## 6 Dealing with Potential Breaches of the Data Protection Policy

6.1 All security breaches must I be reported to the Data Protection Officer immediately.

6.2 The Data Protection Officer will inform the individual(s) to whom the personal data relates that there has been a potential breach.

6.3 The Data Protection Officer will then conduct an investigation to establish the extent and seriousness of the alleged breach.

6.4 The Data Protection Officer will prepare a report on the potential breach for submission to the Principal, with recommendations for further action, if appropriate.

6.5 The Information Commissioner's Office will be informed, if appropriate.

6.6 Disciplinary action may be taken against members of staff or students for any such breach of data protection, under the relevant College policy.

## 7 Student Obligations

7.1 Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc. are notified to personal tutors and/or the Student Records Office and/or the Programme Management Office as appropriate.

7.2 Students who use the College computer facilities may, from time to time, process personal data. If they require further clarification, they should contact the data controller.

## 8 Rights to Access Information

8.1 Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College "Access to Information" form (Appendix 2) and give it to the data controller or their personal tutor or the Information Services office.

8.2 In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached.

8.3 This service is free of charge except

a) where a request from a data subject is manifestly unfounded or excessive; in which case the data controller may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or
b) refuse to act on the request.

8.4 The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

8.5 All requests from the police for the release of personal data should be directed to the Data Protection Officer, who will make the appropriate arrangements. A log of any such requests will be kept.

## 9 Publication of Riverside College Information

9.1 Information that is already in the public domain is exempt from the current Data Protection Legislation. It is the College policy to make relevant information available to the public but it should be noted that the College internal phone list is not considered to be a public document.

9.2 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller.

## 10 Subject Consent

10.1 The College must only process personal data on the basis of one or more of the lawful bases set out in the Current Data Protection Legislation, which include consent. Consent is only valid if it is given by a positive statement or positive action. Data subjects must be easily able to withdraw consent at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if the personal data of an individual will be processed for a different and incompatible purpose which was not disclosed when the individual first consented.

10.2 Sometimes it is necessary to process information about a person's health, welfare, disciplinary, criminal convictions, race, gender and family details. This personal data is described in the Current Data Protection Legislation as 'special

category data'. The College needs to process special category data be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equality and diversity policy. When processing special category data or criminal convictions data, the College will usually rely on a legal basis for processing other than explicit consent or consent if possible. Where explicit consent is relied on, a privacy notice must be issued to the data subject to capture explicit consent

10.3 You will need to evidence consent captured and keep records of all consents in accordance with the [Data Protection Guidelines] so that the College can demonstrate compliance with consent requirements.

## 11 Examination Marks

Students will be entitled to information about their marks for both course work and examinations at no charge. However, this may take longer to provide than other information. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or if all books and equipment have not been returned to the College.

## 12 CCTV Recordings

CCTV recordings are also to be considered as personal data for the purposes of the Data Protection policy and as such are subject to the same safeguards as any other source of personal data. CCTV data will be processed in accordance with the [CCTV policy]

## 13 Retention of Data

13.1 Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

13.1 The College will keep some forms of information for longer than others. Details of the length of time that particular documents will be retained is contained within the College's Data and Document Retention Policy.

13.2 In general, all information about staff will be kept for 10 years after a member of staff leaves the College. Some information however about staff will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Details of the length of time that particular documents will be retained is contained within the College's Data and Document Retention Policy.

## 14 Conclusion

Compliance with the current Data Protection Legislation is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to the College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns

about the interpretation or operation of this policy should be directed to the Data Protection Officer.

**APPENDIX 1**

## The Data Protection Officer and the Designated Data Protection Officer/s

The College, as a body corporate, is the data controller under the Data Protection Act, and is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day to day matters.

The College designated 3 data controllers. They are:
Deputy Principal, Finance and Resources
Head of Systems Development and Funding (in respect of student records)
Head of Human Resources (in respect of staff records)

**APPENDIX 2**

The College Access to Information Form which satisfies the College's Data Protection Policy is to be found overleaf.

Riverside College
Widnes & Runcorn

## ACCESS TO INFORMATION

This form satisfies the requirements of the College's Data Protection Policy

| YOUR DATA | |
|---|---|
| All persons requiring Access to Personal Data in line with the College Data Protection Policy should provide proof of identity. | |
| Reference Number (if known) | |
| Surname | |
| Forenames | |
| Date of Birth | |

| TO BE COMPLETED BY COLLEGE STAFF | | |
|---|---|---|
| Proof of Identity Checked | Please Tick as appropriate | |
| | YES | NO |
| Member of Staff Signature | | |
| Member of Staff Name (Please Print) | | |
| Date | | |

| SUPPLEMENTARY INFORMATION |
|---|
| Please describe briefly below what data you wish to access and sign the declaration below |
| |

| **DECLARATION:** The information I have supplied on this form is correct as far as I am aware. | |
|---|---|
| Signature<br>(person applying for data access) | |
| Date | |