Data Protection Policy

PURPOSE: To inform staff, students and visitors of the Solihull College (the "College") Data Protection Policy and how to request access to data.

SCOPE: This policy applies to all staff, contractors and students.

RESPONSIBILITY: The Director, Risk Control and Compliance is responsible for this Policy.

LEGAL CONTEXT: Data Protection Act 1998 (The "Act")

Data Protection Statement of Intent

1. This policy applies to all employees (permanent and temporary), students, board members, contractors and other users of Solihull College's personal data.

2. The College processes personal and confidential data about its employees, students, employment applicants, board members and tenants. All individuals have a right to privacy under the Data Protection Act 1998.

3. This policy sets out how the College protects and promotes the rights of individuals and groups. It identifies the information that is to be treated as confidential and the procedures for collecting, storing, handling and disclosing such information.

4. This policy will ensure that the College complies with the fair processing code regarding the collection and use of the data collected.

5. This policy will ensure that all persons processing personal data on behalf of the College receive adequate and periodical awareness training to ensure that they understand their contractual and legal responsibility towards the personal information processes in their day to day work.

6. Where students are required to process the personal data of individuals as part of their course of study, specific awareness training will be provided as part of their course induction.

7. To ensure the effective application of the Principles of the Act, the College will ensure that there is a nominated data protection officer within the management structure with the specific responsibility for data protection.

8. The College will ensure that management controls are in place to:

- maintain an accurate and up to date Notification of processing purposes;
- comply with the fair processing code regarding the collection and use of the data collected and ensure the methods for handling and managing personal information collected and processed by the College are periodically reviewed
- maintain the quality and accuracy of data held and processed;
- review the retention periods for which data is reasonably retained;
- fully meet the rights of the data subject regarding data held and processed by the College;
- take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and accidental loss, destruction or damage;
- Protect personal data from transfer outside of the EEA or where such transfer is necessary provide for adequate security of the information.

Data Protection Policy

1 Introduction

The College as a Data Controller needs to process certain information including personal information about its employees, students and other persons to operate effectively and efficiently; for example, the monitoring of performance, achievements, and health and safety. It is also necessary to process personal information so that the College can recruit and pay staff, organise courses and comply with legal obligations to funding bodies and government. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully -whether on paper, in a computer system, or recorded on other media including CCTV. To do this, the College must comply with the Act. In summary, the Act requires personal data to be:

- obtained and processed fairly and lawfully and not to be processed unless certain conditions are met;
- obtained for a specified and lawful purpose and not to be processed in any manner incompatible with that purpose;
- adequate, relevant and not excessive for those purposes;
- accurate and kept up to date;
- kept for no longer than is necessary for that purpose;
- processed in accordance with the data subject's rights;
- kept safe from unauthorised access, accidental loss or destruction;
- transferred to a country outside the European Economic Area only if that country has equivalent levels of protection for personal data.

The Staff Guidelines for Data Protection (see Appendix 1) detail the impact and responsibility of staff and students in relation to each of the eight Data Protection Principles.

All staff and others who process or use any personal information must ensure that they follow these principles at all times. This Data Protection Policy has been drawn up to help in securing compliance with the legislation.

2 Status of the Policy

2.1 This policy is a condition of employment. Staff must abide by the rules and policies made by the College from time to time. Any failures to follow the policy may therefore result in disciplinary proceedings.

2.2 Any member of staff who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with the Director; Risk, Control and Compliance or the College Solicitor. If the matter is not resolved, it may be raised through the grievance procedure which can be found on the college intranet or requested from Human Resources.

2.3 Any student who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with their Course

Tutor in the first instance. If the matter is not resolved, it may be further raised with the Director; Risk, Control and Compliance or the College Solicitor.

3 The Data Controller, the Data Protection Officer and Assistant Data Protection Officers

3.1 The College as a body corporate is the Data Controller under the Act, and the Corporation is therefore ultimately responsible for implementation. However, the designated Data Protection Officer and the Deputy Data Protection Officers will deal with day to day matters.

3.2 The Data Protection Officer for the College is the Deputy Principal.

3.3 The Deputy Data Protection Officers reflect the organisational structure of the College and are as follows: -

- Vice Principal, Human Resources & Student Services
- Vice Principal, Finance
- Vice Principal Teaching, Learning & Assessment
- Director of Risk Control & Compliance
- Assistant Principal Service Industries Faculty
- Assistant Principal STEM Faculty
- Assistant Principal Creative & Professional Faculty
- Senior Director Employment and Skills
- Director of Student Services and Equality
- Information Systems Manager
- Network Manager
- Human Resources Manager
- Finance Manger
- Facilities Manager
- Student Services Manager
- ICT Services Manager
- Clerk to the Corporation
- College Solicitor

It is the responsibility of the Deputy Data Protection Officers to ensure that the provisions of this policy are implemented within their areas of responsibility.

4 Notification of data held and processed

4.1 All staff, students and other users (collectively referred to as data subjects) are entitled to know:

- what information the College holds about them and processes and why;
- how to gain access to the information (see paragraph 8);
- how to keep it up to date;
- what the College is doing to comply with its obligations under the Act.

5 Responsibilities of staff

5.1 All staff are responsible for:

- checking the information that the College sends out from time to time which gives details of information kept and processed about staff;
- 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 the information which they have provided (eg changes of address);
- Informing the College of any errors or changes (the College cannot be held responsible for errors if the member of staff has not brought them to the College's attention).

5.2 If and when, as part of their responsibilities, staff collect information about staff, students or other people, (e.g. about students' course work, opinions about staff / students ability, references to other institutions, or details of personal circumstances), they must comply with the guidelines for staff in Appendix 1.

5.3 All Personal Data Collection forms must be approved by the College Data Protection Officer or the designated Deputy Data Protection Officer. The form will be centrally registered and given a unique version control reference. All internal data collection forms should only ask for personal details relevant to the purpose for the form and should not be excessive.

5.4 The data collected on approved forms and any data made available from the Central IS team must not be used to develop localised data collection and reporting systems.

5.5 Any reporting systems required at a local level must be developed in association with Central IS and approved by the Data Protection Officer. These systems will then become an officially recognised college database and where necessary the College’s notification to the Information Commissioner updated.

6. Data security

6.1 All staff are responsible for ensuring that:

- any personal data which they hold is kept securely;
- Personal information is not disclosed either orally or in writing or accidentally or otherwise, to any unauthorised third party.

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

6.2 The College strives to operate a clear desk policy, when not in use all manual / hard copy personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer;

Wherever possible, all offices should be locked when not occupied.

6.3 Computerised data:

- Is be password protected whilst held within the College network file storage system.
- Should not be stored on 'the Cloud' (i.e. externally hosted storage). The College provides staff with access to their virtual desktop both at work and over the internet so there is no need to use an alternative file storage system outside our own network.
- If there is a justified reason for holding the data on portable devices including USB memory sticks, external hard drives and the hard drives of personal laptops then the device should be encrypted. Encrypted USB memory sticks are available from the Faculty Office and from ICT Services on demand. College laptops are by default encrypted.

Notwithstanding 6.3, The College's Acceptable Use Policy, IT Security Policy and Mobile Devices and Remote Access Policy should be adhered to at all times.

6.4 All staff should ensure that they do not take electronic personal data off College premises.

6.5 When transferring and sharing data with external organisations, such as funding bodies or Auditors, necessary security arrangements must be adhered to using encryption and following appropriate protocols agreed by the Data Protection Officer and the ICT Services Manager.
Staff should note: The sharing of personal information may require a Data Sharing Agreement to be in place. If in doubt, contact the Data Protection Officer or College Solicitor prior to sharing the information.

6.6 At an organisational level the College may elect to use externally hosted systems (Cloud-based systems) to provide its staff and students with services. This practice must only be undertaken by College management following the acceptance of data protection and security assurances from relevant third parties (see 'Guidance on the Adoption of Externally Hosted Services' and the associated 'Externally Hosted Services – Checklist', both available on the College Intranet).
Staff should note: The sharing of personal information may require a Data Sharing Agreement to be in place. If in doubt, contact the Data Protection Officer or College Solicitor prior to sharing the information.

6.7 **Data Loss Incidents:** If you lose any personal information or have files or electronic devices containing personal information stolen you MUST inform the Data Protection Officer, the College Solicitor and the ICT Services Manager

immediately. The College's Incident Management procedures contain further specific advice.

7. Students' 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 in writing using the appropriate change of details form to their tutor.

7.2 Students who use College computer facilities may, from time to time, process personal data. If they do, they must notify the Head of Student Services through their tutor. Any student who requires further clarification about this should contact the Head of Student Services.

7.3 Students on certain courses will process personal information on "clients" as part of their practical experience based work. Tutors will make students aware of their responsibilities under this section as part of the student induction to their course. Students should also ensure they comply with the Guidelines for Students (Appendix 2)

8. Rights to gain access to information

8.1 Staff, students and others have the right to gain access to any personal data that is being kept about them either on computer or in certain files. The College will provide on request to all staff, students and other users a standard form of notification. This will show all the types of data the College holds about them and processes, and the reasons for which it is processed. Any person who wishes to exercise this right should complete the College's 'Access to Information' form and send it to the Deputy Principal. 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 (Appendix 3).

8.2 The College will make a charge of £10 on each occasion that access is requested, although the charge may be waived under certain circumstances agreed by the Data Protection Officer in accordance with agreed protocol obtained from the Data Protection Officer.

8.3 The College aims to comply with requests for access to personal information as quickly as possible and within the statutory deadline of 40 days.

9. Publication of College information

9.1 Information that is already in the public domain is exempt from the 1998 Act. It is the College's policy to make public information in accordance with its approved Publication Scheme, which is reviewed from time to time. In particular the following information will be available to the public for inspection:

- names of College governors

- names of staff (with consent)
- photographs of key staff and governors
- registers of interests
- information shown in the policy statement on access to information (if this contains personal information, then consent may be required)

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated Data Protection Officer or College Solicitor. The College's internal phone and e-mail address lists will not be public documents.

10. Subject consent and Processing Sensitive Information

10.1 In many cases, the College may process personal data only with the written consent of the individual. Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be necessary to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course and a condition of employment for staff. Offers of employment or places on courses may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from the Data Protection Officer or the College Solicitor.

10.2 Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments and regulatory requirements to ensure that staff are suitable for the job, and students are suitable for the courses offered. The College has a duty of care to all staff and students and will take such steps as may be reasonably practicable to make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

10.3 The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need written consent to process it in the event, for example, of a medical emergency.

10.4 All prospective staff and students will be asked to sign Consent to Process form, relating to particular types of information, when an offer of employment or a course place is made. A refusal to sign such a form may result in the offer being withdrawn.

11. Data Subject Information Requests

11.1 All requests received from staff or students or other individuals external to the college for access to personal information should be referred without delay to the Data Protection Officer or College Solicitor.

11.2 Requests for personal information from the police: Sometimes, if the law allows as prescribed within the non-disclosure exemptions, we can or have to, release information about a data subject. The Police may request information quoting s29 of the Data Protection Act which is a “non-disclosure exemption for purposes relating to Crime and Taxation. Solicitors may quote s35 of the Data Protection Act which is an exemption for purposes related to legal proceedings. All such requests MUST be referred to the Data Protection Officer or the College Solicitor without delay to ensure the correct process is followed.

12. Examination marks

Students will be entitled to information about their marks for both coursework and examinations. Information on the exemption on disclosure and release of examination marks can be obtained from the Data Protection Officer.

13. Retention of data

13.1 The College has a separate Data Retention, Archiving and Disposal Policy which details the policy for the retention of data.

14. Transferring of personal or sensitive data via e-mail

14.1 Users should not use the services of the College Internet and / or e-mail to obtain or send material which contravenes the law or published College policies.

14.2 Users are advised that the use of e-mail to send personal data to a third party is expressly forbidden unless prior approval is obtained from the College's Data Protection Officer. All information MUST be appropriately encrypted and password protected, if in doubt seek advice from the ICT Services Manager.

14.3 Users are advised that all e-mails sent from an account is the responsibility of the individual account holder.

14.4 Further information on compliance in this area is detailed in the College's Acceptable Use Policy, IT Security Policy and Mobile Devices and Remote Access Policy

15. Transferring of personal or sensitive data outside of the EEA

Personal data must not be transferred to a country outside the EEA unless that country has equivalent levels of protection for personal data. Therefore, any personal data being sent outside of the EEA must be approved by the Data Protection Officer. This includes all electronic forms of communication; such as personal information being posted on the College's website, the official College's social media accounts (including "You Tube") or held in "the Cloud".

16. Conclusion

Compliance with the 1998 Act is the responsibility of everyone processing personal information on behalf of the College, (including staff and students). Any deliberate breach of the Data Protection policy may lead to disciplinary action being taken, access to College facilities being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer or the College Solicitor.

Appendix 1

Staff Guidelines for compliance with Data Protection

(In accordance with the eight Data Protection principles set out in the Data Protection Act 1998 and referred to in paragraph 1 of this Policy).

1. All staff will regularly process data about students, when completing registers, marking course work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure, through admission and registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the Act. The information with which staff deal on a day-to-day basis will cover categories such as:

    - general personal details such as name and address;
    - details of class attendance, course work marks and grades and associated comments;
    - notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership; and ethnicity or race is sensitive and can only be collected and processed with the student's express consent. If staff need to record this information, they should use the College standard form (eg: for recording information about medical conditions, dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties).

3. All staff have a duty to make sure that they comply with the data protection principles which are set out in the College's Data Protection Policy. All staff may at some stage during their employment with the College and University Centre come into contact with, and process personal and possibly sensitive personal data. It is essential that staff are aware of their responsibilities under the Act and process any such data in accordance with this Data Protection Policy.
   In particular, staff must ensure that records are:

    - Accurate and fair;
    - up-to-date;
    - relevant and not excessive;
    - kept and disposed of safely and securely, and in accordance with College policy.

4. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or in line with this data protection policy.

5. Staff must not disclose personal data to any other member of staff except with the authorisation or agreement of the Data Protection Officer, or in line with this data protection policy.

6 If you lose any personal information or have files or electronic devices containing personal information stolen you MUST inform the Data Protection Officer, the College Solicitor and the ICT Services Manager immediately. The College and University Centre Incident Management procedures contain further specific advice.

7 Before processing any personal data, all staff should consider the following checklist:

Staff checklist for recording data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student or member of staff been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process the information, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Appendix 3

Standard Request Form for Access to Data

I (print name) ……...

Address / Contact Details: ……...

……

Wish to have access to: **Either** (delete as appropriate):

a) All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; ☐

or:

b) Data that the College has about me in the following categories:

- Academic marks or course work details ☐
- Academic or employment references ☐
- Disciplinary records ☐
- Health and medical matters ☐
- Trade union information (including political) ☐
- Any statements of opinion about my abilities or performance ☐
- Personal details including name, address, date of birth etc ☐

Please tick the appropriate box(es)

I am currently **either** (please delete as appropriate):

a employed at Solihull College; **or**

b enrolled as a student at Solihull College and my student ID number is .....

I understand that I will have to pay a fee of £10 which should be paid at the time the form is submitted.

Signed: ……

Date: ……..

Please submit completed form to the Data Protection Officer at Blossomfield Campus.

This request will not be processed unless this form is signed. The college may request confirmation of ID in certain circumstances.