Title: Data Protection Policy

Type:	Policy
Purpose:	To inform staff, students and visitors of the Solihull College (the "College") Data Protection Policy and how to request access to data purpose of the document
Scope:	All staff, contractors and students.
Responsibility:	The Director of Risk Control and Compliance
Legal Context	General Data Protection Regulation (EU) 2016/679 ("GDPR") Data Protection Act 2018 (The "Act") together "Data Protection Laws"

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 Laws. 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.

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

4. 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.

5. 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.

6. 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.

7. 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 Data Protection Laws. In summary, the Data Protection Laws require personal data to be:

- processed fairly, lawfully and in a transparent manner;
- obtained for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purpose for which it is being processed;
- 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.

These Principles are considered in more detail in the remainder of this policy.

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 Legal Counsel. 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 of Risk, Control and Compliance or the Legal Counsel.

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 Director of Risk Control and Compliance. The Data Protection Officer shall have at least the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

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

- Deputy Principal and Chief Operating Officer (Stratford)
- Vice Principal Human Resources & Student Services
- Vice Principal Finance
- Vice Principal Quality & Curriculum
- Director of Risk Control & Compliance
- Assistant Principal Service Industries Faculty
- Assistant Principal STEAM Faculty
- Executive Director Employment and Skills and IOT
- Director of Student Services
- Director of Funding and Information Systems
- Director of IT
- Human Resources Manager
- Head of Finance
- Head of Estates
- Employer Services Manager
- ICT Services Manager
- Clerk to the Corporation
- College Legal Counsel

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 which is within the overall responsibility and remit of the Data Protection Officer.

4. Basis For Processing Personal Data

4.1 In relation to any processing activity that involves personal data the College will, before the processing starts for the first time, and then regularly while it continues:

4.1.1 Review the purposes of the particular processing activity and identify the most appropriate lawful basis for that processing.

The lawful bases for processing are:

- that the data subject has consented to the processing;
- that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- that the processing is necessary for compliance with a legal obligation to which the College is subject;
- that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
- that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by the College; or
- where the College is not carrying out tasks as a public authority, that the processing is necessary for the purposes of the legitimate interests of the College or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

4.1.2 Except where the processing is based on consent, satisfy itself that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

4.1.3 Document the decision as to which lawful basis applies, to help demonstrate the College's compliance with the data protection principles;

4.1.4 Include information about both the purposes of the processing and the lawful basis for it in the College's relevant privacy notices; and

4.1.5 Where sensitive personal data is processed, also identify a lawful special condition for processing that information (see paragraph 5 below), and document it.

5. Sensitive Personal Data

5.1 Sensitive personal data is personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

5.2 The College may from time to time need to process sensitive personal data. We will only process sensitive personal data if:

5.2.1 We have a lawful basis for doing so as set out in paragraph 4.1.5 above; and

5.2.2 One of the special conditions for processing sensitive personal data applies, namely:

- the data subject has given explicit consent;
- the processing is necessary for the purposes of exercising the employment law rights or obligations of the College or of the data subject;

- the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
- the processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims; or
- the processing is necessary for reasons of substantial public interest.

5.3 Where sensitive personal data is processed, the recipients of any such data will be on a need to know basis

6. Data Privacy Impact Assessments ('DPIAS')

6.1. Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the College is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal data.

6.2. All DPIAs must be reviewed and approved by the Data Protection Officer

7. Individual Rights

7.1 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;
- how to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
- how to restrict the processing of personal data temporarily where the accuracy of the information is contested, or the processing is unlawful (but the data subject does not want the data to be erased), or where the College no longer needs the personal data but the data subject requires the data to establish, exercise or defend a legal claim or where the data subject has objected to the processing (and the College is considering whether the College's legitimate grounds override the data subject's interests).
- what the College is doing to comply with its obligations under Data Protection Laws.

7.2 The College has the following privacy policies**:**

- General Privacy Policy
- Privacy Policy – Students
- Privacy Policy – Staff
- Privacy Policy – Governors

These privacy notices provide details of how these individual rights can be exercised. In most cases, individuals are advised to contact the College's Data Protection Officer.

8 Individual Obligations

8.1 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 (e.g. changes of address or the bank or building society account to which they are paid);
- informing the College of any errors or changes (the College cannot be held responsible for errors if the member of staff has provided inaccurate information and has not brought them to the colleges attention).

8.2 Members of staff may have access to the personal data of other members of staff, students and other clients and suppliers of the College in the course of their employment or engagement. If so, the College expects such members of staff to help meet the College's data protection obligations to those individuals.

8.3 Any member of staff who has access to College personal data must:

- only access the personal data that they have authority to access, and only for authorised purposes;
- only allow others to access personal data if they have appropriate authorisation to do so.

8.4 College Personal Data Collection forms such as enrolment forms, staff application forms, student application forms must be approved by the College Data Protection Officer or the designated Deputy Data Protection Officer. All internal college data collection forms should be approved by either the Data Protection Officer or the Deputy Data Protection Officer and should only ask for personal details relevant to the purpose for the form and should not be excessive.

8.5 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.

8.6 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.

8.7. The College's Data Protection Officer should be contacted if any member of staff is concerned or suspects that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal data, without also one of the conditions in paragraph 5.2.2 above being met;
- access to personal data without the proper authorisation;
- personal data not kept or deleted securely;
- removal of personal data, or devices containing personal data (or which can be used to access it), from the College's premises without appropriate security measures being in place;
- any other breach of this policy or of any of the data protection principles set out in paragraph 1 above.

9 Data security

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

9.1 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.

9.2 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.

9.3 Computerised data:

- is 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 9.3, The College's Acceptable Use Policy, IT Security Policy and Mobile Devices and Remote Access Policy should be adhered to at all times.

- The College's Mobile Devices and Remote access policy covers the use of bring your own devices.

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

9.5 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 Legal Counsel prior to sharing the information.

9.6 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 Legal Counsel prior to sharing the information.

9.7 Staff should ensure that they do not use personal emails or personal cloud storage to transfer or store high risk data.

10 Data Breaches

10.1 A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it**.**

10.2 If you lose any personal information or have files or electronic devices containing personal information stolen you MUST inform the Data Protection Officer, the Legal Counsel and the Director of IT immediately. The College's Incident Management procedures contain further specific advice.

10.3 The College will:

- investigate any reported actual or suspected data security breach;
- where applicable (the ICO has an on line self-assessment to determine the notification requirements **https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment**), make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law; and
- notify the Chair of the Corporation and the Chair of the Audit Committee where a high-risk breach has occurred.

10.4 Central Log

A central log is being maintained for data breaches and also data subject information requests (requests for personal data held by the college).

11. Students' obligations

11.1 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.

11.2 Students who use College computer facilities may, from time to time, process personal data. If they do, they must follow any department protocols when collecting the data which will be solely for learning and educational purposes and notify the Head of Student Services through their tutor. Any student who requires further clarification about this should contact the Head of Student Services.

11.3 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).

12. Rights to gain access to information

12.1 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’s Privacy Policies for staff, students and others 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 contact the College via the mailbox data.protection@solihull.ac.uk

12.2 The College aims to comply with requests for access to personal information as quickly as possible and within the statutory deadline of one month.

13. Publication of College information

13.1 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 key staff
- 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 an objection should contact the designated Data Protection Officer or Legal Counsel. The College's internal phone and e-mail address lists will not be public documents.

14. Data Subject Information Requests

14.1 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 Legal Counsel.

14.2 Requests for personal information from third parties can only be disclosed if justified and fair under the GDPR and Data Protection Act or exemption applies. Sometimes, if the law allows as prescribed within the non-disclosure exemptions, we can or have to, release information about a data subject.

All such requests MUST be referred to the Data Protection Officer, the Legal Counsel or the Vice Principal HR and Student Services without delay to ensure the correct process is followed.

15. Examination marks

15.1 Students will be entitled to information about their marks for both coursework and examinations. Information on the release of examination marks can be obtained from the Data Protection Officer in accordance with legal response times; one month from the date the request was made or the exam results were released. Students have no rights to access to examination scripts, but the comments on the examination scripts are disclosable.

16. Retention of data

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

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

17.1 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.

17.2 Users are advised that the use of email to send personal data to a third party must be sent securely e.g. through a secure portal, encrypted or password protected.
All information MUST be appropriately encrypted and password protected, if in doubt seek advice from the ICT Services Manager.

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

17.4 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.

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

18.1 Personal data must not be transferred to a country outside the EEA unless that country is listed as adequate by the EEA or certain safeguards are implemented. 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 "YouTube") or held in "the Cloud".

19. Compliance with the Policy

19.1 Compliance with the Data Protection Laws 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 Legal Counsel.

Author	Date Created	Approved By	Last Reviewed	Next Review Date
Sam Bromwich	March 2000	Corporation	October 2021	November 2022

Publication:

Staff Hub/Intranet: Y
Website: Y
Student Hub: Y