Personal Data Protection Policy

REF NO. INF-ICT-012

Approved by Senior Leadership Team (SLT)

Strategy/Policy Responsibility: Senior Leadership Team (SLT)	
Date approved	August 2019
Review date	August 2023
Next review date	August 2024

SUTTON COLLEGE PERSONAL DATA PROTECTION POLICY

1. BACKGROUND

1.1 The Data Protection Act 2018 which includes General Data Protection Regulation (GDPR) and is enforceable from May 2018, has replaced the Data Protection Act 1998 as UK personal data protection Law.

1.2 This College personal data protection policy addresses the incorporation into all activities of the College the key principles and requirements of this new regulation.

1.3 Sutton College holds and uses personal data across a range of physical sites, and functional departments, in its information systems and in a variety of formats.

1.4 Personal information is vital to the operations and interests of the College and should be managed in all its forms with care and in compliance with the requirements of the Data Protection Act and UK law.

1.5 This policy should be read in conjunction with specific published procedures and guidelines, available to the public, students and staff, as required.

1.6 Article 4 (1) of the GDPR defines personal data as: 'any information relating 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 name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'.

2. SCOPE

2.1 This policy covers all activities and processes of the College that uses personal information in whatever format.

2.2 This policy relates to all College staff, students and others acting for or on behalf of the College or who are given access to College personal information.

3. GDPR PRINCIPLES, ARTICLES AND RECITALS

3.1 Sutton College will manage the processing of personal information in compliance with the key GDPR principles and its relevant Articles and Recitals, as set out in the full Regulation, and with any relevant supporting guidance issued by the UK Information Commissioner.

3.2 The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. Please follow this link to access the principles on the ICO's website https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/. In order to comply with its obligations, the College undertakes to adhere to these principles:

3.2.1 Process personal data fairly and lawfully. The College will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

3.2.2 Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose. The College will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3.2.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed. The College will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

3.2.4 Keep personal data accurate and, where necessary, up to date. The College will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the College if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the College to ensure that any notification regarding the change is noted and acted on.

3.2.5 Only keep personal data for as long as is necessary. The College undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means The College will undertake a regular review of the information held and implement a weeding process. The College will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

3.2.6 Process personal data in accordance with the rights of the data subject under the legislation. Individuals have various rights detailed in GDPR Articles 15-21 which will be respected and supported by the College. These include:

(a) Right of Subject Access
(b) Right of Rectification
(c) Right of Erasure ('right to be forgotten')
(d) Right to Restriction of Processing
(e) Right of Data Portability
(f) Right to Object to Processing

3.2.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data. All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The College will ensure that all personal data is accessible only to those who have a valid reason for using it.

The College will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

(a) keeping all personal data in a lockable cabinets and/or lockable offices with key controlled access;
(a) password protecting personal data held electronically;
(b) archiving personal data which is then kept securely (lockable cabinet and/or office with key-controlled access);
(c) placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff;
(d) ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, The College will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

3.2.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The College will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so the College will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the College collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

In addition to these principles, this policy commits the College to compliance with the Articles of the GDPR, its supporting Recitals and any official guidance on personal data protection available from the Information Commissioner's Office (ICO).

The GDPR Recitals and Articles are available here: https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf

For the purposes of this policy, all College staff, agents and contractors are especially directed **to Appendix 1**, which provides references for key GDPR Articles and available ICO guidance.

Appendix 1 includes the GDPR text defining 'sensitive personal information' categories, now known as 'special category' personal data in the GDPR.

4. PERSONAL INFORMATION COLLECTION AND USE

4.1 Collection and use of personal information will be kept to a minimum to meet required purposes. Where it is possible to use anonymous information collection to fulfil required purposes, in research or general service feedback for example, these approaches should be encouraged.

4.2 Where personal information is being collected with the intention of using it for direct marketing purposes, individuals will be given the opportunity at the point of collection to refuse consent to direct marketing, in compliance with Electronic Communications Regulations.

4.3 The College will apply approaches to personal information capture, use and maintenance that helps ensure personal information quality and reduces risks of inaccuracy and unnecessary duplication.

4.4 The College will create and maintain a Records Management Policy and related Records Retention Schedules to guide required personal information retention and timely destruction.

5. DATA SUBJECT RIGHTS

The 8 fundamental data subject rights are:

5.1 **The right to information.** This right provides the data subject with the ability to ask the College for information about what personal data (about him or her) is being processed and the rationale for such processing.

5.2 **The right to access**. This right provides the data subject with the ability to get access to his or her personal data that is being processed. This request provides the right for data subjects to see or view their own personal data, as well as to request copies of the personal data.

5.3 **The right to rectification.** This right provides the data subject with the ability to ask for modifications to his or her personal data in case the data subject believes that this personal data is not up to date or accurate.

5.4 **The right to withdraw consent**. This right provides the data subject with the ability to withdraw a previously given consent for processing of their personal data for a purpose. The request would then require the company to stop the processing of the personal data that was based on the consent provided earlier.

5.5 **The right to object**. This right provides the data subject with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent, if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a data subject asks that his or her personal data should not be processed for certain purposes while a legal matter is in process.

5.6 **The right to object to automated processing**. This right provides the data subject with the ability to object to a decision based on automated processing. Using this right, a data subject may ask for his or her request (for example, a course approval request) to be reviewed manually, because he or she believes that automated processing of his or her data (e.g. review of attendance) may not consider the unique situation of the data subject.

5.7 **The right to be forgotten**. Also known as *right to erasure*, this right provides the data subject with the ability to ask for the deletion of their data. This will generally apply to situations where a data subject is no longer engaging the services of the College. It is important to note that this is not an absolute right, and depends on the College retention schedule and retention period in line with other applicable laws.

5.8 **The right for data portability**. This right provides the data subject with the ability to ask for transfer of his or her personal data. As part of such request, the data subject may ask for his or her personal data to be provided back (to him or her) or transferred to another controller. When doing so, the personal data must be provided or transferred in a readable format, and following security policies for transfer of personal data.

6. Business Change

The College will consider personal data protection in the context of required business changes and any associated IT changes and initiatives. Compliance to the Data Protection Act 2018 and UK law will be considered fully in relation to business and IT options and changes and will be supported by appropriate project management frameworks and activities, including requirements for data protection impact assessments, as given in Article 35 (see **Appendix 1**).

7. The Protection and Security of Personal Information

7.1 Security breaches will be monitored and subject to appropriate processes, activities and reporting with reference to Article 33 (see **Appendix 1**). The GDPR requires breach reporting to be made to the ICO in a timely manner, within 72 hours if required. Staff should report all personal data breaches as soon as they are discovered.

7.2 Security policies and processes will encompass access to user accounts and the interception of communications for legitimate College purposes (for example to

intercept email containing potentially damaging attachments or viruses) or where required to do so by law. For further details, please see the College's Information Security Policy.

8. Awareness and Training

8.1 The College will provide guidance, support and relevant training on the management of personal information and relevant legislation to all staff, students and those acting for or on behalf of the College. Staff also sign their employment contract which contains clauses regarding data protection and their responsibility for data they process and have access to. They also confirm that they have read and understand the College data protection and computer security policies.

8.2 The College has a legal responsibility as an institution to operate within the terms of the Data Protection Act 2018 but each member of staff or student could also have a personal liability for any unauthorised disclosure they make. Disclosing information outside the terms of the College Policy could result in disciplinary action.

9. Reviews and Continuous Improvement

9.1 Processes for managing personal information, including those that relate to corporate applications such as the Student Records System and HR system, will be periodically reviewed and any recommendations implemented as part of a continuous process of improvement.

9.2 The management of personal information in research will be subject to review, and where appropriate approval of the relevant College group given.

9.3 Compliance to data subject access requests and other formal requests for personal information will be monitored on a monthly basis and appropriate trends recorded and reported to the Director of Finance and Resources, and further reported to the Senior Leadership Team and the Head of IT.

10. Personal Information Management Policy Roles and Responsibilities

10.1 The College Personal Data Protection Policy is agreed by the Senior Management Team (Planning Group) and formally approved by the Senior Leadership Team and the Head of IT.

10.2 The Data Information Services department is responsible for maintaining College Records Management Policy, Records Retention Schedules and all associated policies and training.

10.3 The Head of IT is responsible for the College Information Security Policy.

10.4 The Senior Leadership Team is responsible for:

- Maintaining this policy
- Managing and reporting on formal subject rights requests and other formal requests for personal information

- Providing guidance, awareness, support and training on the management of personal information and relevant legislation
- Liaison with the Information Commissioner's Office on data protection matters
- Supplying analysis, information and views to external bodies in relation to personal data protection as thought appropriate

11. Wider Personal Information Management Roles and Responsibilities

11.1 All College managers are responsible for ensuring general awareness and compliance with this policy in their areas.

11.2 All College managers will ensure that the records of processing activities required by Article 30 (see **Appendix 1**) are wholly adequate and kept up-to date, and can be made available to the Senior Leadership Team on request.

11.3 All staff, students, contractors and consultants who handle personal information, for or on behalf of the College, are responsible for its safety, security and compliance to the provisions of the Data Protection Act 2018.

11.4 Any security breach or data damage or loss that affects personal information should be reported to dataprotection@suttoncollege.ac.uk. Security breaches and data damage or loss should be reported as soon as anything is discovered.

11.5 Mishandling of personal information in any instance could lead to a disciplinary investigation and additionally could be a breach of the law. Staff are advised to seek assistance and guidance from the Data Information Services department and the Senior Leadership Team if they have specific concerns in this area.

11.6 Data subject rights and information requests are granted in law and all staff involved in such requests should ensure requested information is made available to the Data Information Services department in a timely and accurate manner. It should be noted that it is an offence to conceal, alter or destroy personal information to prevent it from being processed or reviewed that been the subject of a data rights request.

APPENDIX 1 – GDPR RECITALS AND ARTICLES, AND ICO GUIDANCE

For the GDPR recitals and articles see:

https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf

For ICO guidance related specifically to the GDPR see:

https://ico.org.uk/for-organisations/data-protection-reform/

The following is a brief GDPR Articles list that may be of special interest to this policy

Article 4: Definitions

Key definitions of the GDPR including: personal data; processing; profiling; 'pseudonymisation'; controller; processor; consent; personal data breach; genetic data; biometric data; cross border processing; information society service; and other terms.

Article 5: Principles relating to data processing

As described in point 4 of this policy.

Article6: Lawfulness of processing

The six possible legal basis for lawful processing: consent, contract, legal obligation, vital interests, public task, and legitimate interests

Article7: Conditions for Consent

The conditions of evidence that need to be recorded for consent, clear presentation of the matter needing consent, rights of withdrawal and issues of consent in relation to the performance of a contract.

Article 8: Child consent and information society services

The processing of the personal data of a child must be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing will be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Article 9: Processing of special categories of personal data

Under the Data Protection Act 1998 these were known as 'sensitive personal data'. The
GDPR now says:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,

data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

If this data is being processed, there needs to be lawful basis (article 6) on which the data is collected and processed.

Article 13: Information to be provided where personal data are collected from the data subject

The specific information to be given to a data subject when their personal information is collected:

- Identity of the main data controller: Sutton College (London Borough of Sutton)
- Contact details for personal data protection issues: John Thorburn, Head of IT
- Purpose of the processing
- Recipients of the data
- Details of any transfers of data to a third country or international organisation and the related adequacy decision or safeguards in place and how to obtain a copy of these details
- Retention period
- Information rights
- How to withdraw consent if that is the basis of processing
- Right to lodge a complaint
- Legal basis of processing
- Any automated decision making, including profiling

Articles 15 - 21: Data Subject Rights

As described in point 6 of this policy.

Article 22: Automated individual decision making, including profiling

Right not to be subject to automated decision making processing unless based on explicit consent or limited circumstances.

Article 24: Responsibility of the controller

The specific reference to implementing, “appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation…” and the importance of appropriate data protection policies and adherence to approved codes of conduct.

Article 25: Data protection by design and default

The article that introduces the concept of privacy by design, at the time of determination and implementation, and by default, by use of such things as data minimisation and ‘pseudonymisation’ to ensure the requirements of the GDPR are met.

Article 28: Processor

A key Article for consideration of those who offer or undertake the processing of personal information on behalf of the College. Processors must be able to meet all the requirements of the GDPR.

Article 30: Record of processing activities

The College and, where applicable, the College's representative, shall maintain a record of processing activities under its responsibility.

Article 32: Security of Processing – Full Article

1. The College will have appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. The College and processor shall take steps to ensure that any natural person acting under the authority of the College or the processor who has access to personal data does not process them except on instructions from the College, unless he or she is required to do so by Union or Member State law.

Article 33: Notification of a personal data breach to the supervisory authority

When a data breach is likely to result in a risk to the rights and freedoms of natural persons, it must be reported no later than 72 hours to the ICO after the College has become aware of it.

Article 34: Communication of a personal data breach to the data subject

In some cases the College must communicate data breaches to those affected.

Article 35: Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

APPENDICES

Education & Skills Funding Agency Privacy Notice

All students can view the Education & Skills Funding Agency privacy notice each time they enrol with Sutton College. It is on the enrolment form, both hardcopy and also when enrolling online.

It can also be found online if the student has not yet enrolled with Sutton College: https://www.gov.uk/government/publications/lrs-privacy-notices

Retention Schedule

We only retain documents for the time required for the services we provide and also according to guidance provided by funding, education, and all other agencies we are accountable to. You can contact dataprotection@suttoncollege.ac.uk for more information

Records Management Policy

The College's Records Management Policy can be found at https://www.suttoncollege.ac.uk/college/missions-policies/

Right to access requests

All right to access (subject access requests) can be sent to dataprotection@suttoncollege.ac.uk

Data Breach Reports

Any data breaches must be reported at dataprotection@suttoncollege.ac.uk