South Thames Colleges Group

Carshalton College | Kingston College | Merton College | South Thames College

Data Protection Policy

Contents

Introduction

1 South Thames Colleges Group (the Group) is committed to the protection of sensitive personal data, and its proper processing in accordance with data protection law and regulations. The current legal framework includes the Data Protection Act 2018, and the UK General Data Protection Regulation (GDPR), effective from May 2018. It applies to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

2 The Group is required to keep personal information about employees, students and other users to enable it to carry out its core functions, for example, to allow it to monitor performance, achievements, health and safety, recruitment etc. The Group also has legal obligations to submit data to government funding bodies / agencies. To comply with the law, information must be used fairly, stored safely and not be disclosed to any person unlawfully.

3 This document sets out the overarching policy principles. The detailed application within the Group is set out in the **Group Data Protection Procedures: Guidance for Staff**.

Policy Principles

4 The Group will ensure compliance with the data protection principles that set out the main responsibilities for organisations. These require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Original date produced: 24/05/2018	Last updated: 23/08/2022
Updated by: Dan Thornton, Director of MIS	Next review date: 30/09/2024

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

Lawful Processing

5 The Group will ensure that all data processing is undertaken lawfully. A minimum of one of the following lawful bases will apply whenever the Group processes personal data. The lawful basis for processing the data must be determined **in advance**. As a public entity (e) is likely to apply to the majority of processing undertaken by the South Thames Colleges Group:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Individual Rights

6 The General Data Protection Regulations enshrine the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

7 The Group and all staff who process or use any personal information must ensure that fully respect and comply with these rights at all times. Further details on the rights and required compliance are set out in the Group Data Protection Procedures.

Accountability and Governance

8 South Thames Colleges Group will development and maintain comprehensive but proportionate governance measures. These measures will minimise the risk of breaches and uphold the protection of personal data. These measures will enable the Group to demonstrate compliance with the data protection principles, and will include:

a) appropriate technical and organisational measures that ensure and demonstrate compliance (e.g. staff training, internal audits of processing activities, and reviews of internal HR policies);

b) maintaining relevant documentation on processing activities;

c) ensuring the appointment of a suitable data protection officer;

d) implementation of measures that meet the principles of data protection by design and data protection by default. Including:

- data minimisation;
- pseudonymisation;
- transparency.

9 Consideration will be given to creating and improving security features on an ongoing basis, and the use of data protection impact assessments where appropriate.

Contracts

10 Where South Thames Colleges Group in its capacity as “Data Controller” uses a “Processor” (a third party who processes personal data on behalf of the Group), a written contract will be in place, and will

include as a minimum the following requirement on the processor:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and

Documentation

11 The documentation of processing activities is a new requirement under the GDPR. The Group is required to maintain a record of its processing activities, covering areas such as processing purposes, data sharing and retention.

12 As a minimum the following information will be documented:

- The name and contact details of the organisation (and where applicable, of other controllers, representatives and the data protection officer).
- The purposes of processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of technical and organisational security measures.

Data Protection Officer

13 As a public authority the Group is required to appoint a Data Protection Officer (DPO). The DPO assists in the monitoring of internal compliance, informs and advises on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Appointed DPO:

- The Deputy Chief Executive Officer (DCEO) is the appointed DPO and registered with the Information Commissioners Office (ICO).
- The DCEO is supported by the Director of MIS and Director of IT. Both act in advisory roles as experts of their respective areas of management.

Requirements for the DPO:

- The DPO reports directly to the highest level of management and is given the required independence to perform their tasks.
- The DPO will be involved in a timely manner, in all issues relating to the protection of personal data.
- The DPO will be sufficiently well resourced to be able to perform their tasks.
- The DPO will not be penalized for performing their duties.
- Any other tasks or duties assigned to the DPO will not result in a conflict of interests with their role as a DPO.

Tasks of the DPO:

- The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.
- The DPO will provide advice and the information on data protection obligations.
- The DPO acts as a contact point for the ICO. They will co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.
- The DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO:

- The DPO is easily accessible as a point of contact for our employees, individuals and the ICO.
- Contact details of the DPO will be publicised and communicated to the ICO

Security

14 South Thames Colleges Group will ensure that all personal information is held with appropriate security and that all staff are aware of their obligations, in particular that:

- any personal data which they hold is kept securely

- personal information is not disclosed to any unauthorised third party

- Personal information will be:

    - kept in a locked filing cabinet; or
    - in a locked drawer; or
    - if it is computerised, be password protected; or
    - stored only on a disk which is itself secure

- Personal information will not be:

    - taken offsite unless its business critical to do so – Head of School/Service approval should be sought
    - if it must be taken offsite it must be kept secure at all times
    - Not disclosed to any unauthorised third party, either orally or in writing, accidentally or otherwise

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

International Transfers

16 GDPR, tailored by the Data Protection Act 2018, sets out specific conditions for the transfer of personal data outside of the UK. This is unlikely to be relevant to the activities of South Thames Colleges Group. In the event that a potential requirement for the international transfer of data is identified specific guidance and permission should be sought from the Data Protection Officer.

Personal Data Breaches

17 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

18 Where a personal data breach has occurred South Thames Colleges Group will assess the likelihood and severity of the resulting risk to people's rights and freedoms. This will include consideration of whether this breach will result in result in:

"physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

19 Breaches that impact on a person's "rights and freedoms" will be notified to the ICO within 72 hrs, as set out in the Data Protection Procedures.

20 Where a decision is taken by the Data Protection Officer not to notify the ICO, relevant information must be retained, along with documentation in support of the decision not to report.

21 The report to the ICO will include the following:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

22 Where it is not possible to provide the information in full within 72 hours, it is permitted to provide it in phases provided there is not undue delay.

Status of the Policy

23 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 Group rules and policies. Any failure to follow the policy can therefore result in disciplinary proceedings.

24 Any member of staff who considers that the policy has not been followed in respect of personal data should raise the matter with the Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

Review

25 The policy will be subject to annual review. The review will be initiated by the Data Protection Officer.

Access to the policy

26 The policy will be published on the Group Intranet and website.