



Data Protection Policy

Version:	3.2	Document Title:	Data Protection Policy
Author:	Ansar Mahmood	Date:	15/09/2026
Approved:	Executive Board	Due for review:	15/09/2028

SIGNIFICANT CHANGES FOLLOWING REVIEW

Page Number or Heading Name	Details of significant change	Changes made by
Whole Document	Updated to UK GDPR and Data Protection Act 2018	Whole Document
Governance	Replaced GDPR Owner references with Data Protection Officer	Governance
Roles & Responsibilities	Introduced Information Asset Owner responsibilities	Roles & Responsibilities
International Transfers	Removed Privacy Shield and EEA transfer provisions	International Transfers
Data Subject Rights	Updated to current UK GDPR rights	Data Subject Rights
Consent	Clarified lawful basis and use of consent	Consent
Information Asset Register	Added ROPA requirements	Information Asset Register
Security	Updated technical and organisational controls	Security

1. Introduction and Scope

- 1.1 South Essex Colleges Group is committed to complying with the law in respect of personal data and the protection of rights and freedoms of individuals whose information it collects and processes. This includes learners, staff, employers, governors, contractors, volunteers, suppliers and others.
- 1.2 This policy applies to all departments that process personal data.
- 1.3 All employees are required to adhere to this policy including those mentioned in 1.1 above.
- 1.4 No third party may access information without having entered into a data sharing agreement.
- 1.5 Any breaches will be investigated by the relevant authorities.
- 1.6 Background to the General Data Protection Regulation ('GDPR')

South Essex Colleges Group (SECG) processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated information rights legislation.

- 1.7 The purpose of data protection legislation is to protect the rights and freedoms of individuals and to ensure that personal data is processed lawfully, fairly and transparently.
- 1.8 SECG recognises that personal information is a valuable asset and is committed to ensuring that personal data is processed securely, responsibly and in accordance with legal requirements and good practice Definitions used by the organisation (drawn from the GDPR)
- 1.9 Article 4 definitions

Personal data – 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 a 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.

Special categories of personal data – 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.

Data controller – the natural or legal person, public authority, agency or other

body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines A child is generally considered under the age of 13 for online consent services under Article 8 UK GDPR. Educational processing will normally rely upon Public Task or Legal Obligation rather than consent. The processing of personal data relating to children may rely upon a variety of lawful bases depending on the activity being undertaken. Consent will only be used where it is the most appropriate lawful basis.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed

on a functional or geographical basis.

2. Policy statement

- 2.1 South Essex Colleges Group is committed to protecting the rights and freedoms of individuals and processing personal data in accordance with UK GDPR, the Data Protection Act 2018 and associated information rights legislation.
- 2.2 Compliance with data protection legislation is supported by this policy together with associated procedures, standards and guidance including the Data Breach Procedure, Subject Access Request Procedure, Privacy Notices, Records Retention Schedule and Information Security Policies.
- 2.3 This policy applies to all processing of personal data undertaken by SECG, including information relating to learners, apprentices, higher education students, staff, governors, contractors, employers, suppliers, visitors and other stakeholders.
- 2.4 The GDPR and this policy apply to all of South Essex Colleges Group personal data processing functions, including those performed on customers, clients, employees, suppliers and partners' personal data, and any other personal data the organisation processes from any source.
- 2.5 Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to South Essex Colleges Group's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.
- 2.6 This policy applies to all Employees/Staff and any other interested parties of South Essex Colleges Group such as outsourced suppliers. Any breach of the GDPR will be dealt with under South Essex Colleges Group's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
- 2.7 Partners and any third parties working with or for South Essex Colleges Group, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by South Essex Colleges Group without having first entered into a data sharing or data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which South Essex Colleges Group is committed, and which gives South Essex Colleges Group the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

- 3.1 South Essex Colleges Group is the Data Controller for the personal data it processes.
- 3.2 The Executive Board has overall accountability for ensuring that SECG complies with data protection legislation and maintains effective information governance arrangements.
- 3.3 The Executive Sponsor for Information Governance is responsible for promoting compliance, ensuring appropriate resources are available and supporting the implementation of information governance arrangements across SECG.
- 3.4 Data Protection Officer (DPO) is responsible for:
- Monitoring compliance with UK GDPR and the Data Protection Act 2018.
 - Providing advice on data protection obligations.
 - Advising on Data Protection Impact Assessments.
 - Acting as a contact point for the Information Commissioner's Office (ICO).
 - Supporting data subject rights requests.
 - Monitoring data protection risks and reporting significant issues to senior management.
 - Promoting awareness and training.
- 3.5 Information Asset Owners (IAOs) are responsible for:
- Understanding and documenting the information assets under their control.
 - Ensuring personal data is processed lawfully and securely.
 - Reviewing retention requirements.
 - Supporting DPIAs where required.
 - Reporting data protection risks and incidents.
- 3.6 Managers are responsible for ensuring that staff within their areas comply with this policy and related procedures.
- 3.7 Employees, Workers, Contractors and Governors - All individuals working for or on behalf of SECG are responsible for:
- Complying with this policy.
 - Protecting personal data.
 - Reporting data breaches promptly.
 - Completing mandatory information governance training.
 - Following SECG security requirements.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. South Essex Colleges Group's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing”, for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The ICO provides guidance on 'Privacy notices, transparency and control' here: <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparency – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

South Essex Colleges Group's Privacy Notice Procedure and Privacy Notice is available on the college website.

The specific information that South Essex Colleges Group will provide to the data subject must, as a minimum, include:

- 4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
- 4.1.2 the contact details of the Data Protection Officer;
- 4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- 4.1.4 the period for which the personal data will be stored;
- 4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating

- to exercising these rights, such as whether the lawfulness of previous processing will be affected;
 - 4.1.6 the categories of personal data concerned;
 - 4.1.7 the recipients or categories of recipients of the personal data, where applicable;
 - 4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
 - 4.1.9 any further information necessary to guarantee fair processing.
- 4.2 Personal data can only be collected for specific, explicit and legitimate purposes Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of South Essex Colleges Group's GDPR register of processing. Privacy Procedure GDPR sets out the relevant procedures.
- 4.3 Personal data must be adequate, relevant and limited to what is necessary for processing
 - 4.3.1 The Data Protection Officer is responsible for ensuring that South Essex Colleges Group does not collect information that is not strictly necessary for the purpose for which it is obtained.
 - 4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.
 - 4.3.3 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by resource owners to ensure that collected data continues to be adequate, relevant and not excessive
- 4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
 - 4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
 - 4.4.2 It is also the responsibility of the data subject to ensure that data held by South Essex Colleges Group is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

- 4.4.3 Employees/Staff should be required to notify South Essex Colleges Group of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of South Essex Colleges Group to ensure that any notification regarding change of circumstances is recorded and acted upon.
- 4.4.4 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- 4.4.5 On at least an annual basis, the Data Protection Officer or controllers will review the retention dates of all the personal data processed by South Essex Colleges Group, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.
- 4.4.6 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If South Essex Colleges Group decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.
- 4.4.7 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.
- 4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
 - 4.5.1 Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
 - 4.5.2 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods

defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

- 4.6 Personal data must be processed in a manner that ensures the appropriate security The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of South Essex Colleges Group's controlling or processing operations.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on South Essex Colleges Group itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate IT technical measures, the Data Protection Officer will work with the Head of IT (and second data controller) to consider the following:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymization and anonymization;
- Identifying appropriate international security standards relevant to South Essex Colleges Group.
- Appropriate Data Loss Protection technologies.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout South Essex Colleges Group;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security training completion;
- Physical access controls to electronic and paper based records;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- When transferring personal data internationally, SECG will utilise UK GDPR compliant transfer mechanisms including UK Adequacy Regulations, International Data Transfer Agreements (IDTAs) and the UK Addendum where applicable.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

South Essex Colleges Group will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident management response plans.

The ICO has published guidance on Accountability and Governance here <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/>

5. **Data subjects' rights**

SECG recognises and supports the rights of individuals under UK GDPR. Individuals have the right to:

- Be informed about how their personal data is used.
- Access their personal data.
- Request correction of inaccurate personal data.
- Request erasure of personal data where applicable.
- Request restriction of processing.
- Receive personal data in a portable format where applicable.
- Object to processing in certain circumstances.
- Object to direct marketing.
- Challenge decisions based solely on automated decision making where applicable.

SECG will respond to requests in accordance with statutory timescales and applicable legal requirements.

Requests relating to personal data should be directed to the Data Protection Officer.

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO)

6. Consent

- 6.1 Consent will only be relied upon as a lawful basis where it is appropriate and where the requirements of UK GDPR can be satisfied.
- 6.2 Consent must be freely given, specific, informed, unambiguous, capable of being withdrawn at any time.
- 6.3 SECG will maintain records demonstrating where consent has been obtained.
- 6.4 Individuals have the right to withdraw consent at any time and will be informed how to do so.
- 6.5 In most educational and employment-related processing activities, SECG will rely upon Public Task, Contract or Legal Obligation rather than consent.
- 6.6 Where Special Category Personal Data is processed, SECG will ensure that an appropriate Article 9 condition is identified and documented.

7. Security of data

- 7.1 All Employees, Workers, Contractors and Governors are responsible for ensuring that any personal data that South Essex Colleges Group holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by South Essex Colleges Group to receive that information and has entered into a confidentiality or data sharing agreement.
- 7.2 SECG will implement appropriate technical and organisational measures to protect personal data, including:
 - Access controls and role-based permissions.
 - Multi-factor authentication where appropriate.
 - Endpoint protection and anti-malware controls.
 - Secure backup and recovery arrangements.
 - Data Loss Prevention technologies where appropriate.
 - Encryption of portable devices and sensitive data.
 - Security monitoring and incident detection.
 - Staff awareness and mandatory training.
 - Physical security controls.
 - Supplier security due diligence.
- 7.3 Security controls will be reviewed periodically to ensure they remain effective and proportionate to risk.
- 7.4 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:
 - in a lockable room with controlled access; and/or

- in a locked drawer or filing cabinet; and/or
 - if computerised, password protected in line with corporate requirements in the Access Control Policy and/or
- 7.5 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of South Essex Colleges Group. All Employees/Staff/Students are required to sign an agreement at Network Logon on the Staff and Student Acceptable Use Agreement before they are given access to network logons and organisational information of any sort, which details rules on screen time-outs. Time-outs are 10 minutes as per the National Cyber Security Centre's recommendations.
- 7.6 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation.
- 7.7 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste.' Hard drives of redundant PCs are to be removed and data wiped or destroyed as required by our disposal form.
- 7.8 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8. Disclosure of data

- 8.1 South Essex Colleges Group must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of South Essex Colleges Group's business.
- 8.2 Requests to disclose personal data must be assessed against an appropriate lawful basis and authorised by the relevant Information Asset Owner and, where appropriate, the Data Protection Officer. All disclosures must be recorded and supported by appropriate documentation.

9. Retention and disposal of data

- 9.1 South Essex Colleges Group shall not keep personal data in a form that permits identification of data subjects for longer than is necessary, in relation to the purpose(s) for which the data was originally collected.
- 9.2 South Essex Colleges Group may store data for longer periods if the personal

data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

- 9.3 The retention period for each category of personal data are set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations South Essex Colleges Group has to retain the data.
- 9.4 South Essex Colleges Group's data retention and data disposal procedures will apply in all cases.
- 9.5 Personal data must be disposed of securely in accordance with the storage limitation and integrity/confidentiality principles under Article 5 UK GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

10. Data transfers

International Transfers

South Essex Colleges Group will ensure that any international transfer of personal data complies with Chapter V UK GDPR and will utilise the following and where appropriate, Transfer Risk Assessments (TRAs) will be undertaken before transfers are made.

:

- UK Adequacy Regulations
- International Data Transfer Agreements (IDTAs)
- UK Addendum to Standard Contractual Clauses
- Transfer Risk Assessments where required.

11. Information Asset Register and Records of Processing Activities

- 11.1 SECG maintains Records of Processing Activities (ROPA) and an Information Asset Register to demonstrate compliance with accountability requirements.
- 11.2 Information Asset Owners are responsible for maintaining accurate records relating to the information assets under their control.
- 11.3 SECG will undertake Data Protection Impact Assessments where processing is likely to result in a high risk to the rights and freedoms of individuals

- 11.4 The Data Protection Officer will provide advice and oversight in relation to DPIAs and information governance risks.
- 11.5 Information assets, processing activities and associated risks will be reviewed periodically to ensure continued compliance with UK GDPR and the Data Protection Act 2018.
- 11.6 Significant risks, breaches or compliance concerns will be escalated through SECG governance arrangements and, where appropriate, reported to the Executive Board.
- 11.7 The ROPA will be reviewed at least annually by the Data Protection Officer in conjunction with Information Asset Owners.