Data Protection Statement
&
Data Privacy Policy
Dual Document

Review Date: May 2025
Next Review: May 2028

SIGNIFICANT CHANGES FOLLOWING REVIEW

Page Number or Heading Name	Details of significant change	Changes made by
Whole document	Rewording of job titles to make responsibilities clearer	Pete Daly – October 2024
Whole document	Merged the Data Privacy Policy and Data Protection Policy into one single clear concise document. Followed feedback from OU CMA project.	May 2025

Alternative formats of this document are available upon request. Please contact the Data Protection Officer at dpo@southessex.ac.uk.

South Essex Colleges Group

Date: May 2025

Change Summary: This policy merges the Data Privacy Statement and Data Protection Policy into one comprehensive document. All content has been retained, reformatted, and extended to ensure compliance with accessibility, version control, and transparency requirements.

Contents

1. Introduction

This combined Data Protection and Privacy Policy outlines how South Essex Colleges Group ("we", "our", "us") collects, uses, stores, and protects personal data. It fulfils our legal obligations under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and informs individuals whose data we process ("you", "your") about their rights.

South Essex Colleges Group is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. This policy outlines the responsibilities and obligations of the College in handling personal data and sets out the conditions under which data must be managed. This policy applies to all staff, students, contractors, commercial clients, and anyone else whose personal data the College may process.

2. Definitions

This section provides key terminology used in this document, consistent with Article 4 of the UK GDPR:

- **Personal Data**: Any information relating to an identified or identifiable natural person. This includes names, identification numbers, location data, online identifiers, or any information relating to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.
- **Special Categories of Personal Data**: Sensitive personal data which includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used to identify an individual), health information, and data concerning a person's sex life or sexual orientation.
- **Processing**: Any operation performed on personal data, whether automated or not, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, erasure, or destruction.
- **Data Controller**: The entity that determines the purposes and means of the processing of personal data.
- **Data Processor**: Any party that processes personal data on behalf of the data controller.
- **Data Subject**: The individual to whom the personal data relates.
- **Data Protection Officer (DPO)**: A designated individual responsible for overseeing the College's data protection strategy and implementation.
- **Profiling:**
  Automated processing of personal data to evaluate or predict personal aspects (e.g. work performance, health, preferences). Data subjects have a right to object and to be informed about profiling.

- **Personal Data Breach:**
  Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Controllers must report breaches to the ICO within 72 hours and to data subjects where there's a high risk.
- **Child:**
  Any individual under 16 (or lower if permitted by UK law). Processing children's data lawfully requires parental or guardian consent, with reasonable efforts to verify it.
- **Filing System:**
  Any structured set of personal data accessible according to specific criteria, whether centralised or dispersed.
- **Establishment:**
  The place in which a controller makes the main decisions on purposes and means of processing. Non-EEA controllers must appoint an EU-based representative.
- **Third Party:**
  Any natural or legal person, public authority, agency or body other than the data subject, controller, processor or authorised staff.

3. What Information We Collect

South Essex Colleges Group collects a wide range of personal data in the course of its operations. This includes, but is not limited to:

- Personal identifiers such as full name, date of birth, gender, national insurance number, student or staff identification number, and contact details including address, telephone number, and email address.
- Academic and professional qualifications, prior educational history, details of previous employment, and references.
- Financial information including bank details, tuition fees, bursary and scholarship details, and payroll data for staff.
- Medical and health-related information such as disabilities, dietary requirements, health conditions, and medical history where relevant for pastoral care, safety, or compliance with legal obligations.
- Criminal record information, including any relevant convictions or DBS checks required for safeguarding purposes.
- Behavioural and attendance data, assessment results, disciplinary records, and academic performance indicators.
- Technical data such as IP addresses, login data, browser type, and activity logs collected through College systems and websites.
- Visual and audio data through CCTV, lecture recordings, and video calls.
- We collect standard internet log information and visitor behavior patterns (page views, session duration, referrer URLs), in anonymised form, to analyse and improve our websites.

This data is collected through various channels including application and registration forms, during the course of studies or employment, from previous institutions or employers, and through digital interactions with College systems and platforms.

4. How Information is Collected

Personal data is collected through a variety of channels depending on the nature of the interaction with the College:

- **Directly from individuals**: When a person fills out application forms, enrols in a course, signs an employment contract, engages with commercial services, or otherwise provides personal details during College interactions.
- **Through electronic systems**: The College utilises various IT systems and digital platforms that log data during their use. These include Virtual Learning Environments (VLEs), HR and Finance systems, email servers, library management systems, and attendance tracking tools.
- **Via communication channels**: Personal data may be collected when individuals correspond with the College via email, telephone, or social media, or when participating in surveys and feedback processes.
- **From third-party sources**: Previous education providers, current or former employers, government agencies, and statutory bodies may provide personal data to the College, particularly in contexts such as admissions, job applications, safeguarding investigations, or legal compliance.
- **Automatically via technology**: Website cookies, network monitoring tools, and campus access control systems may collect data automatically when users engage with online or physical College environments.
- **Simple Information-Request Handling:** All enquiries (email, telephone, web-form, in person) are logged in our enquiry system. You'll receive an acknowledgment, and we'll follow up to ensure your request is resolved and maintain an audit trail.

5. Lawful Basis for Processing

Processing of personal data by South Essex Colleges Group will always rely on at least one of the lawful bases for processing under Article 6 of the UK GDPR. These are:

- **Performance of a contract**: Processing is necessary for the performance of a contract to which the data subject is party, such as the enrolment and delivery of a study programme, or an employment contract.
- **Legal obligation**: Processing is necessary for compliance with a legal obligation to which the College is subject. This includes statutory reporting, safeguarding, or financial audits.
- **Consent**: Where the College asks for explicit permission to process personal data for one or more specific purposes, and such consent is freely given and can be withdrawn at any time.
- **Vital interests**: Processing is necessary in order to protect the vital interests of the data subject or another person, particularly in cases of medical emergencies.
- **Public task**: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

- **Legitimate interests**: The College may process personal data for its legitimate interests or those of a third party, provided that such interests are not overridden by the rights and freedoms of the data subject.
- **Detailed Consent Requirements**: Consent must be freely given, specific, informed and unambiguous, signified by a clear affirmative act. Silence, pre-ticked boxes or inactivity do not constitute consent. Consent for special-category data must be explicit and documented. You can withdraw consent at any time without affecting prior processing.

In the case of special category data, processing will comply with Article 9 of the UK GDPR and will be justified by additional lawful conditions, such as the necessity for employment obligations, the protection of vital interests, or explicit consent.

6. Use of Your Data

The College uses personal data for a variety of purposes across its educational, administrative, and commercial operations. The nature of the use will depend on the relationship between the College and the data subject. Uses of data include, but are not limited to:

- **Educational administration**: Managing applications, enrolments, registration, timetables, academic assessments, and certification. Data is essential to maintaining accurate records of student progress, attendance, examination results, qualifications awarded, and for the purposes of progression and graduation.
- **Support services**: Delivering services such as counselling, learning support, careers guidance, mentoring, safeguarding, and wellbeing services. Processing is required to ensure that the College can respond to the personal needs of students, particularly where it concerns health or disability.
- **Employment administration**: Managing employment records, payroll, performance appraisals, and compliance with employment legislation. This also includes pre-employment checks and DBS verifications where required by law.
- **Financial transactions and support**: Administering payments, bursaries, grants, and other financial entitlements. Financial data is processed for the effective and lawful management of College funds and compliance with funding agency rules.
- **Communications**: Contacting data subjects in response to queries or communications and sending important administrative or academic information. In specific cases, data may also be used for marketing and promotional purposes, where prior consent has been obtained.
- **Research and development**: Analysing data for the purpose of service improvement, internal audits, institutional reporting, and compliance with inspection and regulatory requirements.
- **Security and IT operations**: Monitoring use of the College's IT systems to ensure compliance with acceptable use policies, as well as ensuring data security and system integrity. CCTV and access control logs are also processed to maintain campus safety and property security.
- **External reporting and audits**: Fulfilling our statutory obligations to report to organisations such as Ofsted, the Department for Education, Education Skills Funding Agency, and other oversight bodies.

- **Graduation & Degree Information**: We publish names, awards and classifications in graduation ceremony booklets, local press and supplier materials. You may withhold consent for your name to appear by notifying us at enrolment. Ceremonies may be recorded and made available online.

In all cases, personal data will only be used in a way that is necessary and proportionate to achieve the stated purpose, and where the lawful basis for processing can be clearly established and recorded.

7. Your Rights

Under the Data Protection Act 2018 and the UK GDPR, individuals have a number of rights with respect to their personal data. These include:

- **Right of access**: You can request a copy of the personal data we hold about you, along with information about how it is processed. This is commonly referred to as a Subject Access Request (SAR). Requests should be sent to the Data Protection Officer (dpo@southessex.ac.uk) with clear detail on the data required.
- **Right to rectification**: You have the right to request that we correct inaccurate or incomplete data.
- **Right to erasure (right to be forgotten)**: In certain circumstances, you may request that your data be erased. This is subject to our legal obligations and retention policies.
- **Right to restriction**: You may request that the processing of your data is restricted while a challenge to the accuracy or use of your data is resolved.
- **Right to data portability**: Where processing is based on consent or contract and is carried out by automated means, you may request to receive your data in a structured, commonly used format.
- **Right to object**: You can object to processing where it is based on public task or legitimate interests. We will stop processing unless we have compelling legitimate grounds to continue.
- **Right to withdraw consent**: If we are processing your data based on consent, you can withdraw this at any time.
- **Right not to be subject to automated decision-making**: You have the right not to be subject to a decision based solely on automated processing, including profiling.
- **Right to Object to Harmful Processing**: You may object where processing is likely to cause you damage or distress (separate from marketing objections).
- **Right to Lodge a Dispute**: You can ask the ICO or other supervisory authority to investigate any alleged GDPR breach.

All rights requests will be handled in line with the College's Subject Access Request Procedure. In general, we aim to respond within one month, with a possible extension to three months for complex cases. You also have the right to lodge a complaint with the Information Commissioner's Office if you believe your data rights have been infringed.

8. Breach Notification Procedure

1. Contain and mitigate the incident immediately.

2. Notify the DPO within 24 hours of discovery.
3. The DPO will report to the ICO within 72 hours of breach occurring if there is a risk to individuals rights and freedoms.
4. The DPO will inform affected data subjects without undue delay if there is high risk.

9. Internal Responsibilities

South Essex Colleges Group assigns clear roles and responsibilities regarding data protection and information governance:

- **Data Protection Officer (DPO)**: The DPO is a designated member of the senior management team responsible for ensuring overall compliance with data protection legislation. The DPO develops and implements the College's policies, oversees risk assessments and DPIAs, and acts as the point of contact with the ICO.
- **Managers and Supervisors**: All individuals in leadership roles are expected to promote a culture of data protection compliance. They must ensure that personal data processed within their departments is handled in accordance with College policies and procedures.
- **All Employees**: Each employee has a responsibility to protect personal data. Staff must ensure that data they handle is accurate, up-to-date, secure, and used only for its intended purpose. Failure to comply with data protection policies may result in disciplinary action.
- **Third-Party Contractors and Partners**: External parties who have access to College data are required to sign data sharing or confidentiality agreements. These agreements must align with the College's data protection standards and allow for audit and oversight of their data handling practices.
- **Register of Processing Activities**: The DPO maintains a RoPA, reviewed at least annually, and available to the ICO on request.
- **Data Protection Impact Assessments**: DPIAs are mandatory for any high-risk processing (large-scale special-category data or new technologies). They must be completed before launch, escalated to the DPO, and, if significant risks remain, to the Executive Committee.

Training is mandatory for all staff with access to personal data. Compliance with data protection procedures is monitored through regular reviews, audits, and incident response protocols.

10. Security Measures

The College is committed to maintaining the confidentiality, integrity, and availability of all personal data it processes. A range of technical and organisational measures are employed to achieve this goal, including but not limited to:

- **Access control**: Systems are configured to grant access to personal data only to those staff members who require it for their roles. Password policies, user authentication, and audit logs are enforced across College systems.
- **Physical security**: All manual records are stored in secure, lockable storage units within restricted-access areas. Visitors to buildings must sign in and be accompanied.

- **IT and cyber security**: Computers and mobile devices are protected with firewalls, antivirus software, and encryption where required. Automatic time-outs and screen locking are enabled, and use of USB and other removable media is restricted.
- **Secure disposal**: Paper records are disposed of using confidential waste bins and shredding. Electronic data is securely wiped or destroyed according to the Secure Disposal of Storage Media Procedure.
- **Remote working safeguards**: Employees authorised to work off-site are required to follow strict guidelines, including using College-issued, encrypted devices and VPNs where applicable.

Security measures are assessed regularly through risk reviews, vulnerability assessments, and external audits. The DPO and Cyber Security Manager are jointly responsible for coordinating the College's data protection risk posture.

11. Sharing Information

The College only shares personal data when there is a clear lawful basis to do so, and where such sharing supports educational, administrative, or statutory functions. Data may be shared internally and externally as follows:

- **Internal sharing**: Between departments within the College, including academic staff, support services, finance, and safeguarding teams, to ensure students and staff receive appropriate support and services.
- **Government bodies and regulators**: Including the Department for Education, Ofsted, Education and Skills Funding Agency, HMRC, and the Home Office. This may be for regulatory, funding, audit, or visa compliance purposes.
- **Service providers**: External organisations contracted to provide services on our behalf (e.g., IT support, payroll processors, accommodation providers). Data sharing is controlled by contracts and subject to appropriate due diligence.
- **Educational and placement partners**: Including universities, employers offering placements, and other institutions to whom students may transfer or from whom we receive students.
- **Parents, carers, and next of kin**: Only where explicit consent is given or where there is a vital interest (e.g., in medical emergencies).
- **Survey organisations**: For research purposes such as the National Student Survey or Destination of Leavers from Higher Education surveys, in accordance with HESA guidance.

All sharing of personal data is governed by formal agreements and is subject to strict access controls. Information will not be sold or rented to third parties. In each instance, we will only share the minimum amount of data necessary for the stated purpose.

12. International Data Transfers

In certain circumstances, South Essex Colleges Group may transfer personal data to countries outside of the United Kingdom or the European Economic Area (EEA). Such transfers will only occur if one or more of the following safeguards or legal mechanisms are in place:

- **Adequacy Decisions**: The European Commission or the UK government has determined that the third country ensures an adequate level of data protection equivalent to that provided under the UK GDPR.
- **Standard Contractual Clauses (SCCs)**: Contracts incorporating clauses approved by the European Commission or the UK Information Commissioner's Office that impose data protection obligations on the recipient of the data.
- **Binding Corporate Rules**: For multinational organisations, approved internal data protection policies that are legally binding and enforceable.
- **Privacy Shield**: For transfers to the United States, data may be transferred to organisations that are certified under the UK Extension to the EU-U.S. Data Privacy Framework, as appropriate.
- **Explicit Consent**: Where none of the above safeguards apply, data may be transferred with the explicit informed consent of the data subject, with a clear explanation of the potential risks.

All international transfers of data are subject to thorough risk assessments and must be approved by the Data Protection Officer. These transfers must comply with the data minimisation principle, and only essential data will be transferred.

13. Retention and Disposal of Data

South Essex Colleges Group retains personal data for no longer than is necessary to fulfil the purpose for which it was collected or to comply with legal, regulatory, or contractual obligations. The retention periods are defined in the College's Retention of Records Procedure.

Generally, most personal data is retained for a period of six years following the end of an individual's relationship with the College, unless longer retention is justified by academic archiving, alumni engagement, or specific regulatory requirements. Academic records, such as award details and transcripts, may be retained indefinitely to support requests for confirmation of qualifications.

When data is no longer required, it is disposed of securely:

- **Paper records** are shredded and disposed of as confidential waste.
- **Electronic records** are permanently deleted or rendered unreadable via certified data destruction tools.

Data disposal must always be documented, and staff are responsible for ensuring they comply with disposal procedures. Breaches of the data disposal protocol may result in disciplinary action.

14. Use of Cookies and Web Data

The College's websites use cookies to improve user experience, analyse web traffic, and personalise content. A cookie is a small file stored on the user's computer which helps analyse web traffic or lets users know when they visit a particular site.

Cookies are used to:

- Remember preferences and settings
- Understand how the website is used
- Improve functionality and design
- Support analytics and marketing efforts (where consent is given)

Users are informed about cookies upon visiting the website and can accept or decline their use. Declining cookies may affect site functionality. Cookie usage is compliant with the Privacy and Electronic Communications Regulations (PECR) and the UK GDPR. Users can manage cookie settings via their browser preferences at any time.

Users do not miss out on any content by declining cookies, these are for technical functionality only.

Links From Our Site:

Our website may link to third-party sites. We have no control over their privacy practices – please review their policies before providing any data.

15. Marketing Communications and Consent

South Essex Colleges Group may contact individuals regarding programmes, events, news, or services offered by the College. These communications will only be sent to individuals who have explicitly opted in to receive marketing content.

Consent for marketing may be collected via:

- Web forms
- Event registrations
- Direct communication and application processes

Individuals can withdraw consent at any time by:

- Emailing marketing@southessex.ac.uk
- Writing to the Marketing Team at the College's main campus address

We will not share or sell your personal data to third-party marketers. All marketing campaigns are subject to internal approval and are conducted in line with the College's Marketing and Communications Policy.

16. Commercial Services, Unions and Surveys

The College operates a number of commercial services such as Hair and Beauty salons. Customers engaging with these services provide personal data necessary to deliver the requested services (e.g., appointment details, health information relevant to treatments). This data is used strictly for the provision and administration of services and related communication.

Additionally, the College works with the Students' Union and may share limited student data (e.g., name, email, course information) to enable Union membership management. Students have the right to opt out of Union-related data sharing by notifying the College during registration.

Participation in national surveys, such as the National Student Survey (NSS) and the Graduate Outcomes Survey, is part of our statutory obligations. Contact details may be shared with third-party survey contractors only for the purpose of administering these surveys. Contractors are required to delete data once the survey is completed. Participation is voluntary, and students can opt out if they wish.

17. Complaints and Contact Information

South Essex Colleges Group takes all data protection concerns seriously. If you have any concerns about how your personal data is being used or wish to raise a complaint, please contact our Data Protection Officer:

Data Protection Officer
South Essex Colleges Group
Luckyn Lane Campus
Basildon
Essex, SS14 3AY
Email: dpo@southessex.ac.uk

If you are not satisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):
Website: www.ico.org.uk
Phone: 0303 123 1113

18. Changes to this Policy

We review this policy regularly and may update it to reflect changes in legislation, guidance, or our internal practices. Significant changes will be communicated to staff, students, and other stakeholders through appropriate channels.

The current version of the policy is published on our website.
Last Reviewed: May 2025
Next Review Due: May 2028