



South Gloucestershire and Stroud College

Data Privacy & Protection Policy

**If you would like this document in an alternate format
Please contact the Human Resources Department**

Prepared by:	Gavin Murray
Job Title / Role:	Data Protection Officer
Ref. No.: Q/P 141 (To be entered by Quality Office)	Date of this version: 01 September 2018 Review date: 20 May 2020 * (Must be at least 1 year) Please note: if the document has details relating to legislation or government guidelines, the following must be added to the Review Date: (subject to any legislative change) Upload to External College website? Yes Upload to e-Campus? Yes
Approved by:	SGS College Corporation
Date of Approval:	10 th October 2019

Completed by:		
Gavin Murray	Assistant Principal, Quality & Performance	09/09/2019
I have read the guidance document: Completing a Policy Impact Assessment?		✓
If this policy has been up-dated, please tick to confirm that the initial impact screening has also been reviewed:		✓

EQUALITY AND DIVERSITY IMPACT ASSESSMENT	
Characteristic	This policy seeks to:
Age	No appreciable impact
Disability	The College will provide appropriate and reasonable support those who require it, to exercise their rights including accessing information
Faith or Belief	No appreciable impact
Gender	No appreciable impact
Race or Ethnicity	No appreciable impact
Orientation	No appreciable impact
Gender reassignment	No appreciable impact
Economic disadvantage	No appreciable impact
Rural isolation	No appreciable impact
Marriage	No appreciable impact
Pregnancy & maternity	No appreciable impact
Carers & care leavers	No appreciable impact
Vulnerable persons	No appreciable impact
Please identify any sections of the policy that specifically seek to maximise opportunities to improve diversity within any of the College's stakeholder groups:	Section 15
Please identify any sections of the policy that specifically seek to improve equality of opportunity within any of the College's stakeholder groups:	
Is there any possibility that this policy could operate in a discriminatory way?	<input type="checkbox"/> <input checked="" type="checkbox"/> * If you have ticked yes (red), which characteristic will be most affected? Choose an item.
If yes please confirm that the Policy has been sent for a full Equality & Diversity Impact Assessment, and note the date:	<input type="checkbox"/> Click or tap to enter a date.

Note: if the policy does not seek to increase diversity or improve equality you should go back and review it before submitting it for approval.

MAPPING OF FUNDAMENTAL RIGHTS	
Which United Nations Convention on the Rights of the Child (UNCRC), Right does this policy most protect:	Art. 17 Access to information Choose an item.
Which Human Right (HRA) does this policy most protect:	Art. 8 Right to private & family life Choose an item.

DATA PROTECTION & PRIVACY BY DESIGN SCREENING	
Tick to confirm that you have considered any data protection issues as part of the design and implementation of this policy; and, that implementing this policy will not result in the collection, storage or processing of personal data outside of official College systems:	✓
Tick to indicated that this policy has or requires a Data Privacy Impact Assessment:	✓

Part 1: General Privacy and Data Protection

1. Introduction

South Gloucestershire and Stroud College (SGS) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

SGS's leadership and management team is fully committed to ensuring continued and effective implementation of this policy and expects all employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

2. Definitions

Personal Data	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.	Process, Processed, Processing	Any operation performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.
Data Controller	South Gloucestershire and Stroud College which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.		
Data Subject	The identified or Identifiable Natural Person to which the data refers. Most likely a Learner, Employee or other Stakeholder whose Personal Data is processed by SGS	Consent	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 relating to him or her.
Third Party processor	An external organisation with which SGS conducts business and is also authorised to, under the direct authority of SGS, Process the Personal Data of SGS Contacts.	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.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.	Automated decision making	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Encryption	The process of converting information or data into code, to prevent unauthorised access.	Anonymised Data	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

3. Application

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with computer software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals. This policy has been designed to establish a baseline standard for the Processing and protection of Personal Data by SGS staff.

This policy does not form part of the formal staff contract of employment, but it is a **condition of employment** that staff abide by the rules and policies made by the College from time to time. Any breach of this policy could, therefore, result in disciplinary proceedings. Any member of staff who considers that this Policy has not been followed, should raise the matter immediately with their line manager.

4. Principles

When Processing Personal Data, SGS staff will adhere to the following principles at all times:

Principle 1: **Lawfulness, Fairness and Transparency**

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, SGS will tell the Data Subject what Processing will occur (transparency), that the Processing will match the description given to the Data Subject (fairness), and that processing will be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: **Purpose Limitation**

SGS shall only collect Personal Data for specified, explicit and legitimate reasons and will not further process data in a manner that is incompatible with those reasons. This means SGS will aim to specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: **Data Minimisation**

SGS will endeavour to ensure that Personal Data is adequate, relevant and limited to what is necessary in relation to the purpose and reasons for which it is processed. This means SGS will not store any Personal Data beyond what is strictly required.

Principle 4: **Accuracy**

Personal Data, held by SGS, shall be accurate and, kept up to date. This means SGS will maintain processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: **Storage Limitation**

SGS shall keep Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is/was Processed. This means SGS will, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: **Integrity & Confidentiality**

SGS shall only process Personal Data in a manner that ensures appropriate security of that data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. SGS will use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: **Transferral**

SGS will only transfer Personal Data to third parties, under contract, when necessary to provide services to our staff and customers or when required to do so by law. SGS will never sell personal data or allow Personal Data to be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Principle 8: **Accountability**

The Data Controller shall be responsible for and be able to demonstrate compliance.

5. The Collection of Personal Data

SGS will only collect Personal Data about a Data Subject if our Mission and the nature of our business purpose necessitates its collection; or if collection is necessary in emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

Personal Data will only be collected from the Data Subject or other public bodies. If Personal Data is collected from someone other than the Data Subject or another Public Body, SGS will inform the Data Subject.

Data Subject Consent

SGS will only obtain Personal Data by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, SGS is committed to seeking such Consent.

Where consent is required SGS commits to:

- **Making appropriate disclosures** to the Data Subject in order to obtain valid Consent;
- **Ensuring the request for consent is presented in a manner which is intelligible** and in an easily accessible form, using clear and plain language;
- **Ensuring the Consent is freely given** (that is: not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract); and,
- **Providing a simple method for a Data Subject to withdraw their Consent at any time.**

In all instances where Consent is sought, it will be: Documenting by date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given; **and the Schedule 2 Checklist will be completed.**

6. Notification of Data Held and Processed

All staff, students and other users of the College are entitled to:

- Know what information the College holds and processes about them and why;
- Know how to gain access to it;
- Know how to keep it up-to-date; and,
- Know what the College is doing to comply with its obligations under Data Protection legislation.

7. Data Use (General Processing)

SGS uses the Personal Data it collects for the following broad purposes:

1. The general running and business administration of SGS College;
2. To provide services and support to SGS customers, and monitor the ongoing administration and management of customer services;
3. To advertise, promote, inform and market to stakeholders, prospective customers and the general public the services offered through SGS College and SGS Group;
4. To monitor a range of activities including performance, achievements and health and safety; and,
5. To ensure compliance with legal obligations to regulatory, awarding and funding bodies and to Her Majesty's Government.

SGS will always consider the use of a Data Subject's personal information from their perspective and whether its use is within their expectations or if they are likely to object.

In other words, if we believe an individual might object to our processing of their personal data, we will not undertake any such processing without legal justification or express consent.

In any circumstance where Consent has not been gained for specific processing SGS will address the following additional conditions to determine the fairness and transparency of that processing, beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing;
- The context in which the Personal Data was collected, in particular regarding the relationship between Data Subject and the Data Controller;
- The nature of the Personal Data, in particular whether Special Categories of data are being processed, or whether Personal Data related to criminal convictions and offences are being processed;
- The possible consequences of the intended further Processing for the Data Subject; and,
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

8. Data use (Necessary Processing)

SGS will only Process Personal Data where that processing is a necessary, targeted and proportionate way of achieving the College's Mission.

By way of general guidance:

- The College's lawful basis for processing Personal Data in respect of employee information is that the processing is necessary to fulfil contractual and HMRC obligations and those within the Keeping children safe in education statutory guidance.
- The College's lawful basis for processing Personal Data in respect of enrolment, funding, awarding body registration, teaching, learner support, performance monitoring and research is that the processing is necessary for the College to perform a task in the public interest and for its official functions; these tasks and functions have a clear basis in law.
- The College's lawful basis for processing Personal Data in respect of alumni relations, internal events, fundraising purposes, direct marketing and marketing research is the pursuit of the College's legitimate interests. (This includes the intra-SGS Group transfer of data for administrative purposes, where those purposes are not detrimental to the rights of the Data Subject)
- SGS College has a lawful basis for further processing, where that processing assists the College in achieving its Mission and is compatible with the purpose for which the data was initially collected.
- SGS College will further process Personal Data for archiving purposes in the public interest and for research and statistical purposes.
- The Processing of Personal Data in respect of keeping children safe in education is a legal obligation under the Education Act 2002.
- When undertaking any major project, concerning the Processing of Personal Data, or considering processing that is likely to result in a high risk to individuals' interests. SGS will undertake a Data Protection Impact Assessment (DPIA); **and the Schedule 5 checklist will be used to determine if a DPIA is required.**

9. Special Categories of Data

SGS will only process Special Categories of data (also known as sensitive data) where the Data Subject has expressly consented to such Processing or where one of the following conditions apply:

1. The Processing relates to Personal Data which has already been made public by the Data Subject;
2. The Processing is necessary for the establishment, exercise or defence of legal claims;
3. The Processing is specifically authorised or required by law (Including the Public Sector Equality Act (Specific Duties) Regulations);

4. The Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent; or
5. Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

10. Marketing

As a general rule SGS will not send promotional or direct marketing material to an SGS Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. **If consent is sought the Schedule 2 Checklist will be completed.**

Any request to carry out a digital marketing campaign or internal event without obtaining prior Consent from the Data Subject must first have it approved by the Data Controller, in consultation with the Data Protection Officer.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject **will be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes.** If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data will cease immediately and their details will be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

11. Responsibilities of Staff

In respect of Personal Data, SGS Staff (including prospective and former staff) should:

1. Check that any information which they provide to the College, in connection with their employment, is accurate and up-to-date;
2. Inform the College of any changes to the information which they have provided e.g. changes of address;
3. Check the information which the College may send out from time-to-time, giving details of information kept and processed about staff;
4. Informing the College of any errors or changes. **The College cannot be held responsible for any errors unless the staff member has informed the College of them.**

In respect of Data Processing

5. Ensure that Personal Data is anonymised or Pseudonymised prior to processing;
6. Prevent unauthorised persons from gaining access to data processing systems in which Personal Data is processed;
7. Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations;
8. Ensure that Personal Data in the course of electronic transmission (or during transport) cannot be read, copied, modified or removed without authorisation;
9. Ensure that personal data is not transferred outside of the College, in any form, which can be read, copied, modified or removed without authorisation;
10. Ensure that access logs are maintained to establish whether, and by whom the Personal Data was entered into, modified on or removed from a data processing system;
11. Ensure that in the case where Processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller (SGS);
12. Ensure that Personal Data is protected against undesired destruction or loss;
13. Ensure that Personal Data collected for different purposes can and is only processed separately;
14. Ensure that Personal Data is not kept for longer than necessary.

If and when, as part of their responsibilities, staff collect or release information about other people, (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the Principals of the Data Protection Act; and **staff should familiarise themselves with Schedule 1: Guidelines for Staff**

This will include:

- Seeking informed consent from the Data Subject; and,
- Undertaking such checks as necessary to verify a person's identity before releasing Personal Information.

12. Learner Obligations

Students must ensure that all personal data provided to the College is accurate and up-to-date. **The College cannot be held responsible for any errors unless Learner has informed the College of them.**

Tutors should be conscious of learners' obligations under the Data Protection Act if Personal Data is being collected and processed using the College's computer services and advise them accordingly.

Learners who use the College's computer facilities may, from time-to-time, process personal data. If they do so they must notify the Data Controller. All students must comply with the College's IT: Acceptable Use Policy.

13. Profiling & Automated Decision-Making

SGS will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by contract (For example: during on-line enrolment or to affect the timely collection of debt).

Where SGS uses profiling and automated decision-making, this will be disclosed to the relevant Data Subjects; and in such cases the Data Subject will be given the opportunity to:

- Express their point of view;
- Obtain an explanation for the automated decision;
- Review the logic used by the automated system;
- Supplement the automated system with additional data;
- Have a human carry out a review of the automated decision;
- Contest the automated decision; or
- Object to the automated decision-making being carried out.

Before engaging in any profiling and automated decision making, SGS will ensure that the data used is accurate and confirm compliance with section 13 with the College's Data Protection Officer.

14. Data Security

All staff are responsible for ensuring that:

- **Any personal data which they hold is kept securely;**
- **Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.**

Staff should note that unauthorised disclosure will usually be a disciplinary matter and, in some cases, may be considered to be gross misconduct.

Personal information should be:

- If it is computerised, stored in an appropriate secure location such as your "My Documents" or an appropriate file share;
- Securely locked away i.e. in a locked filing cabinet or drawer;
- Removable media and portable devices MUST be encrypted and protected by a suitable password;
- NEVER sent by email unless it has been encrypted.

For further information and guidance, please refer to the following policies:

- IT Acceptable Use Policy – Email, Mobile Devices and Users
- IT Security Policy

15. Data Subject Rights

SGS has an established system to enable and facilitate the exercise of Data Subject rights related to:

- Information access (provided through the College's published Data Privacy Notice)
- Objection to Processing
- Objection to automated decision-making and profiling
- Restriction of Processing
- Data portability
- Data rectification
- Data erasure

If an individual makes a request relating to any of the rights listed above, SGS will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subject Rights at a glance:

Purpose of processing	Access Information	Object to processing	Object to automated decisions	Restrict processing	Data portability	Data rectification	Data erasure
Consent	✓	✗ Could withdraw consent	✗ Could withdraw consent	✗	✓	✓	✗ Could withdraw consent
Contract	✓	✗	✗	✗	✓	✓	✓
Legal obligation	✓	✗	✗	✗	✗	✓	✗
Vital Interests	✓	✗	✗	✗	✗	✓	✗
Public task	✓	✗	✓	✗	✗	✓	✗
Legitimate interests	✓	✓	✓	✓	✗	✓	✓

Data Subjects are entitled to obtain, based upon a request made to the College and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data;
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject;
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients;
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period; and,
- The use of any automated decision-making.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Staff, students and other users of the College wishing exercise a Data Subject Right, regarding any personal data that is being kept about them, either on computer or in certain files, are advised to complete the College 'Data Subject Request Form' at Schedule 5 and email it to DataPrivacy@sgscol.ac.uk

16. Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Officer. An investigation of any complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their option, seek redress through mediation or via a complaint to the Information Commissioners Office.

Data Subjects are advised to review the College's Complaints Code of Practice [here](#).

Part 2 Special Provisions

17. Data Requests from the Police

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty; or
- By the order of a court or by any rule of law.

On occasions the College receives requests for information on learners from the Police. The following procedure should be followed:

- The investigating Police Officer should send a DPA (Data Protection Act) form to the College. This should be titled Declaration Form for Data User and should be signed by the Investigating Officer and a Senior Officer. The form should detail the exact information the College is being asked to disclose regarding a learner.
- The Declaration Form for Data User should be sent to the Data Protection Officer for authorisation. Once signed the relevant information can be released.

18. The Use of Photographs and Web pages

Please refer to the Photographic and Visual Media Code of Practice policy [here](#).

19. Electronic communications

The College is committed to securing trust and security in its use of digital marketing and communications. The following specific rules will be followed when processing personal data in the context of electronic communications; and the College will take reasonable care to comply with ePrivacy regulations.

Electronic communications:

- Marketing by electronic means, including marketing calls, texts, emails and faxes;
- The use of cookies or similar technologies that track information about people accessing the College's website or other electronic service.
- The Privacy of stakeholders (not employees) using College communication networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

SGS College will not engage in unsolicited telephone marketing.

SGS College will not engage in unsolicited electronic mail marketing to individuals who have not specifically consented to or opted in to receiving electronic mail.

SGS College will engage in electronic mail marketing to existing learners and stakeholders (including perspective learners who have contacted the College). The College will provide recipients with a simple way to opt out both when we first collect their details and in each instance of marketing activity that we send.

Electronic and digital marketing campaigns, where consent cannot be validly obtained must be authorised by the Data Controller, in consultation with the Data Protection Officer and following the completion of a Data Processing Impact Assessment.

SGS College will, from time to time, use bought-in marketing lists, in each instance we will endeavour to screen lists against our own 'do-not-call' list of people who have previously objected to or opted out of

telephone calls or electronic marketing. SGS College will not sell marketing list unless we have the consent of the listed individuals to do so.

SGS College uses cookies. Where cookies are used the College will tell users of their existence; explain what the cookies are doing and why; and get the person's consent to store a cookie on their device.

Further guidance on electronic communications can be found in the SGS Marketing Policy and Procedure [here](#).

Breaches of ePrivacy will be treated in the same ways a personal data breaches according to section 21 of this policy and the related SGS Breach Notification Procedure.

20. The Data Controller and the Designated Data Controller/s

The 'Data Controller' determines the purposes for which, and the manner in which, personal data is, or are to be, processed. This may be an individual or an organisation, and the processing may be carried out jointly or in common with other persons. The College, as a corporate body, is the Data Controller under the Act, and the Corporation is, therefore, ultimately responsible for the implementation of and on-going compliance with data privacy and protection requirements, processes and procedures.

The College Principal is the 'senior responsible officer' overseeing data privacy and protection issues within the College. Operational authority for data privacy and protection within the College is delegated by the Principal to the Group MIS Director, who also ensures on-going maintenance of the College data privacy and protection Policy.

Data Protection Officer

The Data Protection Officer (DPO) will support the Data Controller to demonstrate transparency, accountability and compliance with the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2017. The DPO will operate with independence, is suitably skilled and granted all necessary authority to report to the 'senior responsible officer' who has direct access to the South Gloucestershire and Stroud College Further Education Corporation.

The Data Protection Officer works with designated data controllers whose duties include:

- Informing and advising SGS and its employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protection provisions;
- Ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (Information Commissioners Office);

'Designated Data Controllers' as detailed below, deal with day-to-day operational matters connected with data privacy and protection and are charged with ensuring compliance within their areas of responsibility:

- All members of the College's Executive and Senior Leadership Team;
- Clerk to the Corporation;
- **Head of Digital and Staff Development;**
- Head of Human Resources;
- **Group Director of IT Services;**
- **Head of Learner Support;**
- Head of Finance;
- **Assistant Principal, Quality and Performance**
- **Assistant Principal, Corporate Development**

Any in-house queries with regard to data privacy and protection should be addressed to the Data Protection Officer or an appropriate designated Data Controller.

21. Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Officer providing a description of what has occurred.

Notification of the incident can be made via e-mail DataPrivacy@sgscol.ac.uk or anonymously by writing to:

Data Protection Officer
SGS Stroud Campus
Stratford Road
Stroud
Gloucestershire
GL5 4AH

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will, depending upon the criticality and quantity of the Personal Data involved, follow the relevant authorised procedure. For critical Personal Data Breaches, the Data Protection Officer will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

22. Relevant references:

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

23. Retention of Data

Personal Data will not be retained for and longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

South Gloucestershire and Stroud College expects that: records and information should only be retained for legitimate business use and must not be retained for longer than is necessary for its lawful purpose.

The College will keep information about students, study and achievements indefinitely in order that we may provide academic references as requested. However, the College will cease processing information about students, study and achievements, except where the data subject consents or for statutory and compliance reasons after 5 years.

In respects of European Social Fund (ESF) funded provision the College will keep all learner data and documents until the end of the document retention period for the 2007 to 2013 ESF programme (31 December 2022); and, for the 2014 to 2020 Programme (until 31 December 2030).

In general, the College will keep information about staff for seven years after a member of staff leaves the College. Some information, however, will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and information required for job references. A non-exhaustive list of information and the College's proposed retention time is contained with the College's Information Asset Register.

The College's Information Asset Register is reviewed, at least annually, and it is the responsibility of Designated Data Controllers to update the Information Asset Register; and no later than 30 days after the acquisition or creation of a new information asset.

Jisc has provided advice on retention for certain groups of administrative records.

Information held for longer than is necessary carries additional risk and cost – SGS will endeavour to ensure that Personal Data and Sensitive Personal Data is up-to-date and maintained for accuracy during the entirety of its retention.

24. Disposal of Data

Once the retention period has elapsed, the College will ensure that any information is, suitably destroyed by secure means, i.e. by shredding or pulping.

Schedule 1: STAFF GUIDELINES FOR DATA PROTECTION

All staff will process data about students on a regular basis, e.g. when marking registers, writing reports or references, as part of a pastoral or academic or supervisory role.

The information with which staff deal on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address;
- Details about class attendance, course work marks and grades and associated comments;
- Notes of personal supervision, including matters about behaviour and discipline.

Staff should **AVOID** processing 'special category data', that is: Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Where processing special category data is unavoidable, it must be anonymised

- Staff **MUST** be able to prove the lawfulness for processing (Article 6 GDPR); and,
- Identify a lawful reason for processing it (Article 9 GDPR)

All staff have a duty to make sure that they comply with the Data Protection principles. In particular, staff must ensure that records are:

- only disclosed as allowed for within the Act
- accurate;
- up-to-date;
- fair;
- kept securely and disposed of safely in accordance with the College Data Protection & Retention Policy.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Has the student been told that the data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Staff Checklist for Disclosing Data

There are some recommended ways of dealing with requests for personal data.

- When dealing with enquiries by telephone it is good practice to offer to call back to a telephone number that is registered on College systems to ensure some measure of authentication or perhaps send them the information by email or letter to an address previously registered with the College
- When dealing with enquiries direct in person, provide identification or verify through photograph held on the College system
- Any third party requests for information must be authorised in writing by the subject and their signature must be checked with the College records

You should always take care to prevent the inadvertent disclosure of personal data (for example a student's attendance at the College) to unauthorised parties.

Enquiries from Police and other Agencies should be referred directly to the Vice Principal and should be accompanied by a "Declaration Form for Data User".

If you are not sure, you should contact a designated Data Controller for clarification.

Schedule 2: Checklist for seeking consent to process Personal Information

This checklist MUST be completed for every consent sought in relation to processing Personal Data

SGS Corporate/ Curriculum function [Choose an item](#). Manager completing this checklist: [Enter name](#)

Asking for consent

We have checked with the Data Controller that consent is the appropriate lawful basis for processing

We have made the request for consent prominent and separate from our terms and conditions

We ask people to positively opt in

We don't use pre-ticked boxes, or any other type of consent by default

We use clear, plain language that is easy to understand

We specify why we want the data and what we're going to do with it

We give granular options to consent to independent processing operations

We have named SGS and any third parties

We tell individuals they can withdraw their consent

We ensure that the individual can refuse to consent without detriment

We don't make consent a precondition of a service

We offer online services directly to children under 13, we only seek consent if we have age-verification and parental-consent measures in place

Not applicable:

Recording consent

We keep a record of when and how we got consent from the individual

We keep a record of exactly what they were told at the time

Records of consent are held: [Choose an item](#). [Add link/location](#)

Managing consent

We will regularly review consents to check that the relationship, the processing and the purposes have not changed

We have processes in place to refresh consent at appropriate intervals, including any parental consents

We make it easy for individuals to withdraw their consent at any time, and publicise how to do so

We act on withdrawals of consent as soon as we can

We don't penalise individuals who wish to withdraw consent

Date when consents will be reviewed: [Click here to enter a date](#).

Completed checklists must be returned to the Data Protection Officer

Schedule 3: Checklist for undertaking diligence on contract formation

This checklist SHOULD be completed for every contract requiring the processing of Personal Data

SGS Corporate/ Curriculum function [Choose an item](#). Manager completing this checklist: [Enter name](#)

Our contracts include the compulsory details and terms:

- The subject matter and duration of the processing
- The nature and purpose of the processing
- The type of personal data and categories of data subject; and
- The obligations and rights of the controller
- The processor must only act on the written instructions of the controller (unless required by law to act without such instructions)
- The processor must ensure that people processing the data are subject to a duty of confidence
- The processor must take appropriate measures to ensure the security of processing
- The processor must only engage a sub-processor with the prior consent of the data controller and a written contract
- The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- The processor must delete or return all personal data to the controller as requested at the end of the contract; and
- The processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state
- The contract must state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and reflect any indemnity that has been agreed.

In addition to the above contractual obligations a processor also their own direct responsibilities under the GDPR. Further detail can be found here:
<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/>

Schedule 4: Is a Data Protection Impact Assessment (DPIA) required?

SGS Corporate/ Curriculum function [Choose an item](#). Manager completing this checklist: [Enter name](#)

Do you intend to process Personal Data [Choose an item](#).

Do you plan to on doing any of the following?

Type of processing	YES	NO
Use systematic and extensive profiling or automated decision-making to make significant decisions about people?	<input type="checkbox"/>	<input type="checkbox"/>
Process special category data or criminal offence data on a large scale?	<input type="checkbox"/>	<input type="checkbox"/>
Systematically monitor (including with CCTV) a publicly accessible place on a large scale?	<input type="checkbox"/>	<input type="checkbox"/>
Use new technologies or innovative technological or organisational solutions?	<input type="checkbox"/>	<input type="checkbox"/>
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	<input type="checkbox"/>	<input type="checkbox"/>
Carry out profiling on a large scale?	<input type="checkbox"/>	<input type="checkbox"/>
Process biometric or genetic data?	<input type="checkbox"/>	<input type="checkbox"/>
Process sensitive data or data of a highly personal nature?	<input type="checkbox"/>	<input type="checkbox"/>
Combine, compare or match data from multiple sources?	<input type="checkbox"/>	<input type="checkbox"/>
Process personal data without providing a privacy notice directly to the individual?	<input type="checkbox"/>	<input type="checkbox"/>
Process personal data in a way which involves tracking individuals' online or offline location or behaviour?	<input type="checkbox"/>	<input type="checkbox"/>
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	<input type="checkbox"/>	<input type="checkbox"/>
Processing of data concerning vulnerable data subjects?	<input type="checkbox"/>	<input type="checkbox"/>
Process personal data which could result in a risk of physical harm in the event of a security breach?	<input type="checkbox"/>	<input type="checkbox"/>
Processing which may involve preventing data subjects from exercising a right or using a service or contract?	<input type="checkbox"/>	<input type="checkbox"/>

SGS will always carry out a DPIA if you plan to do any of the above.

In consultation with the Data Protection Officer we have decided not to carry out a DPIA, for the following reasons:

Schedule 5: SGS Data Privacy & Protection: Data Subject Rights

Please provide the following details, which will help us to process your request.

The completed form can be sent to:

Data Protection Officer
SGS Stroud Campus
Stratford Road
Stroud
Gloucestershire
GL5 4AH

Or emailed to: DataPrivacy@sgscol.ac.uk



SURNAME	
FIRST NAME	
ADDRESS	
TELEPHONE	
EMAIL ADDRESS	

ARE YOU A STUDENT OR A FORMER STUDENT?	YES / NO
WHAT DID YOU STUDY AT SGS COLLEGE	
YEAR OF REGISTRATION	
LEARNER ID NUMBER (IF KNOWN)	
YEAR OF LEAVING / COMPLETION	

ARE YOU A MEMBER OF STAFF OR A FORMER MEMBER OF STAFF?	YES / NO
STAFF ID NUMBER (IF KNOWN)	
WHAT DEPARTMENT(S) DID YOU WORK IN?	
YEARS EMPLOYED AT COLLEGE	
ANY INFORMATION THAT MAY HELP US	

Which Data Subject right(s) does your request relate to?

You do not have to complete this form but it may help us to respond more quickly to your request

I would like to access my Personal Information held by SGS	<input type="checkbox"/>	Please indicate the information you wish to access
		Please indicate the date range for your request (e.g. May 2018 to June 2018)
I would like to object to SGS Processing of my Personal Information	<input type="checkbox"/>	Please indicate the reason for your objection
I would like to object to automated decision-making, by SGS, based upon my Personal Information	<input type="checkbox"/>	Please indicate the automated decision you wish to object to
I would like to restrict Processing of my Personal Information by SGS	<input type="checkbox"/>	Please indicate the information you wish to restrict processing of
I would like to port (transfer) my Personal Information from SGS	<input type="checkbox"/>	Please indicate the information you wish to port and to where
I would like to request rectification of my Personal Information, held by SGS, which I believe to be inaccurate	<input type="checkbox"/>	Please indicate the information you wish to rectify and why
I would like to request erasure of my Personal Data held by SGS	<input type="checkbox"/>	Please indicate the information you wish to erase

SIGNATURE: Date:

NAME (please print):

OFFICE USE ONLY

Date Request received	Request received by
Information Provided	
Signed	
Job Title	Date information provided

9. MANDATORY INITIAL IMPACT SCREENING		
Completed by:		
Gavin Murray	Assistant Principal, Quality & Performance	09/09/2019
I have read the guidance document: Completing a Policy Impact Assessment?		✓
If this policy has been up-dated, please tick to confirm that the initial impact screening has also been reviewed:		✓



EQUALITY AND DIVERSITY IMPACT ASSESSMENT	
Characteristic	This policy seeks to:
Age	No appreciable impact
Disability	The College will provide appropriate and reasonable support those who require it, to exercise their rights including accessing information
Faith or Belief	No appreciable impact
Gender	No appreciable impact
Race or Ethnicity	No appreciable impact
Orientation	No appreciable impact
Gender reassignment	No appreciable impact
Economic disadvantage	No appreciable impact
Rural isolation	No appreciable impact
Marriage	No appreciable impact
Pregnancy & maternity	No appreciable impact
Carers & care leavers	No appreciable impact
Vulnerable persons	No appreciable impact
Please identify any sections of the policy that specifically seek to maximise opportunities to improve diversity within any of the College's stakeholder groups:	Section 15
Please identify any sections of the policy that specifically seek to improve equality of opportunity within any of the College's stakeholder groups:	
Is there any possibility that this policy could operate in a discriminatory way?	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> *
If you have ticked yes (red), which characteristic will be most affected? Choose an item.	
If yes please confirm that the Policy has been sent for a full Equality & Diversity Impact Assessment, and note the date:	<input type="checkbox"/> Click or tap to enter a date.

Note: if the policy does not seek to increase diversity or improve equality you should go back and review it before submitting it for approval.

MAPPING OF FUNDAMENTAL RIGHTS	
Which United Nations Convention on the Rights of the Child (UNCRC), Right does this policy most protect:	Art. 17 Access to information Choose an item.
Which Human Right (HRA) does this policy most protect:	Art. 8 Right to private & family life Choose an item.

DATA PROTECTION & PRIVACY BY DESIGN SCREENING	
Tick to confirm that you have considered any data protection issues as part of the design and implementation of this policy; and, that implementing this policy will <u>not</u> result in the collection, storage or processing of personal data outside of official College systems:	✓
Tick to indicated that this policy has or requires a Data Privacy Impact Assessment:	✓