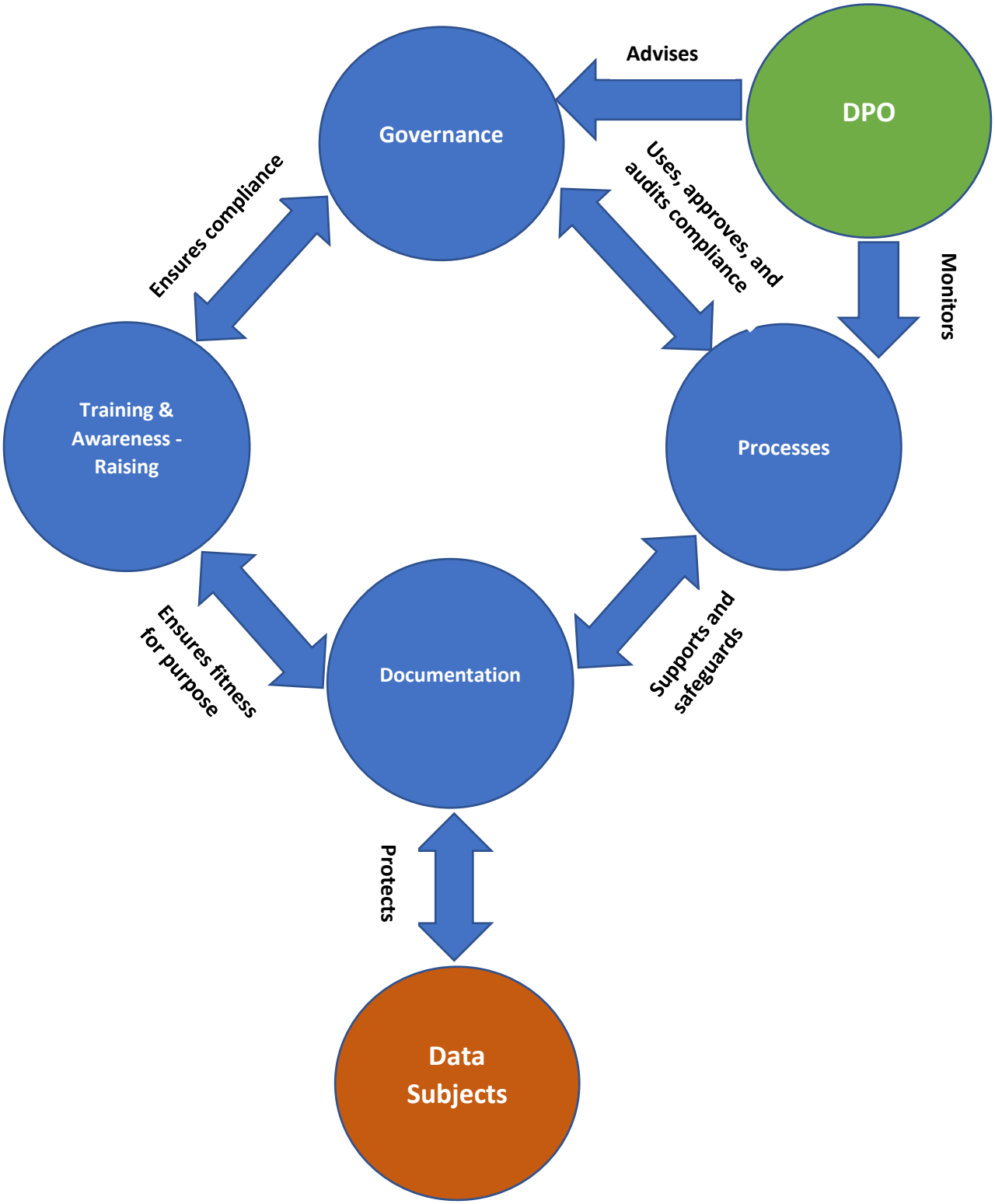
DATA PROTECTION POLICY FRAMEWORK

At Sir George Monoux, College (the College), we are committed to protecting the privacy of our data subjects whether they study, are an employee, an alumnus, a partner, a contractor or a supplier. At all levels of the College, we are obliged to do our best to protect the personal information of our data subjects regardless of who they are and we will only use and keep their personal details for the reason(s) or purpose(s) that they gave their details to us. Below is a representation of our policy framework for to data protection.



Governance

Governance is key to fulfilling our commitment to data protection for our data subjects. Data Protection Governance means having an overview of decision-making guidelines and the processes used by people. From managers to our operational staff, we have people making decisions and helping to deliver on our decisions to fulfil our commitment to data protection. Our governance structure consists…

1. The Senior Leadership Team act as the Data Controller, supervised by the Governing Body.
2. Data Protection Officer
3. Data Protection Group consisting of all team managers, each representing their team as the Information Asset Owner (IAO)
4. Data Protection Champions are members of staff in each team who support the IAO to promote good practices on information handling and provide support to other staff with regards to compliance with UK GDPR/DPA 2018
5. The Teams include Curriculum

To improve and maintain our governance structure we will have:

1. Termly review/update meetings between our SLT and the DPO
2. Termly review/update meetings of the Data Protection Group
3. 'On Demand' meetings, as and when necessary, between the DPO and teams, individuals, groups of individuals, etc. for advice and support and to ensure our committed focus on data protection is carried through

From these meetings, decisions and actions are made and agreed to ensure that there are no lapses in delivering on our commitment to keep safe and secure personally identifiable information of our data subjects.

Processes

Processes are our practices or procedures, i.e. what we do, how we do them and with what we do them to keep personally identifiable information safe and secure. Processes are run and delivered by people from across our staff structure. Processes differ in context as some are college-wide, e.g. Data Subject Access Request, while some are local to teams, e.g. taking the registers in a classroom.

Training & Awareness-Raising

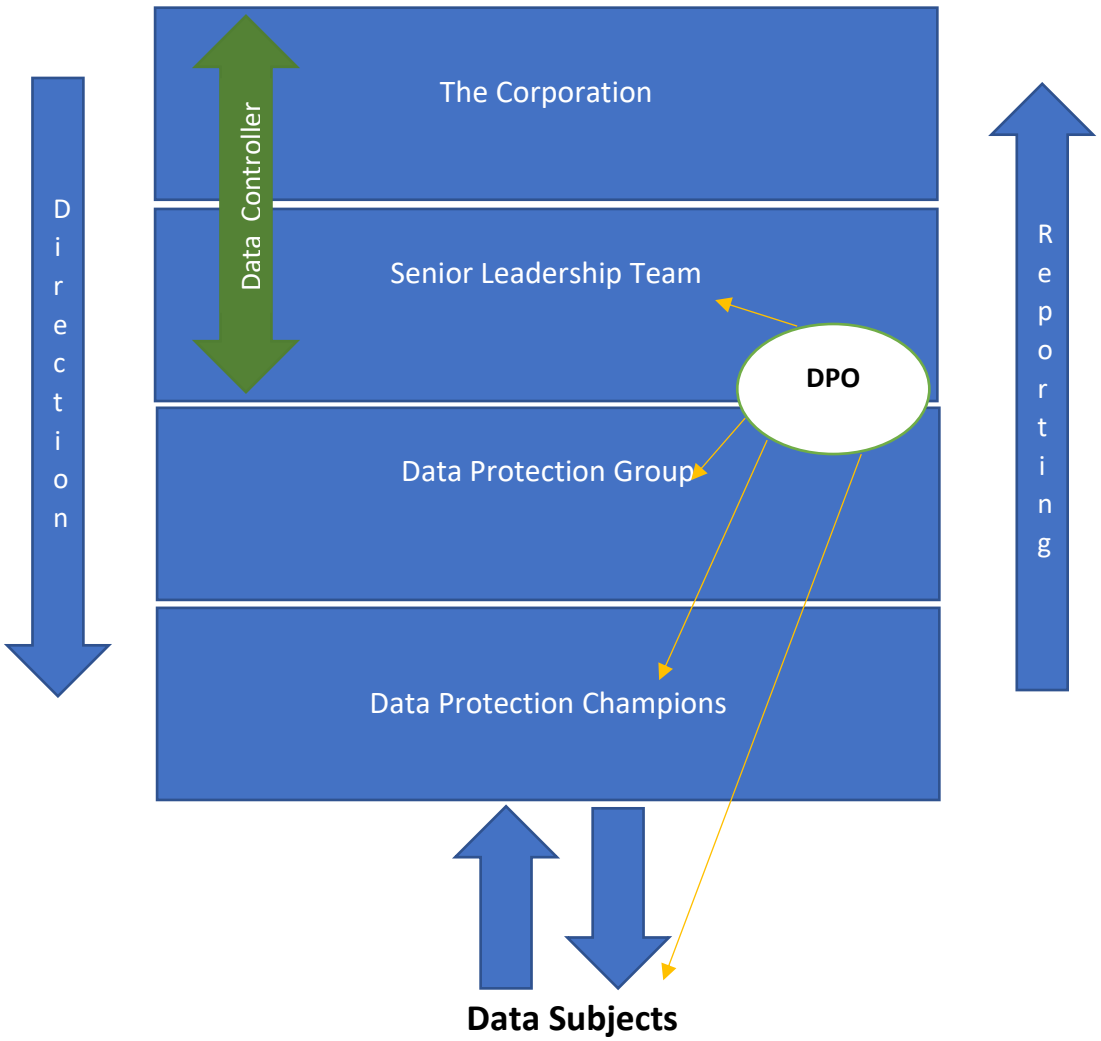
Training and awareness-raising are key to ensure that people are informed, stay informed and have the necessary skills and have due regards to handling personally identifiable information. Our training and awareness-raising effort follow an approach that includes:

1. All Staff Briefing
2. Data Protection training at staff induction
3. Data Protection training at student induction
4. Team time with the DPO
5. Training sessions that are requested based on specific topics or for specific purposes
6. Provision of training content or resources – digital and otherwise
7. Online training platform provided for 'anywhere' 'any time' 'any device' access to training resources
8. Training can be face-to-face, online self-directed or online trainer-directed
9. Training can be for an individual or a group of people

Documentation

Documentation evidences our policies, processes and procedures or what we have committed to do, how we do them and with what we do them to keep personally identifiable information safe and secure. Our documents include the SGMC - Data Protection Policy Framework, SGMC – Data Protection Guidelines, etc.

A Functional View



Data Controller

The College as Data Controller is represented by the SLT with supervision from the Governors. Together, they set the statement of intent for data protection for the College. The vision is a picture of a preferred position that the College should be with regards to data protection; that is that the College should be fully compliant with the UK GDPR/DPA 2018. Getting to that preferred position means that the College will take an approach that shows commitment and focus which is the strategy developed with support from the Data Protection Group to fulfil the vision.

Data Protection Officer

The DPO interfaces with every level in the framework including data subjects and the Information Commissioner's Office (ICO), not represented in the framework. The DPO exists to inform and advise the

College and employees who carry out processing, of their obligations pursuant to the UK GDPR/DPA 2018; to monitor compliance with the UK GDPR/DPA 2018 and the policies of the College in relation to the protection of personal data; is the SME (Subject Matter Expert) on data protection and data privacy; delivers training and awareness-raising sessions, and is the point of contact for the ICO and to co-operate with the ICO as and when necessary.

Data Protection Group

The Data Protection Group consists of all College Team Managers, each representing their team in the Group and are the Information Asset Owner (IAO) for their team. Together with the SLT and the Corporation, they develop the strategy to help deliver the vison for data protection in the college. The Group also determines the tasks, operations or what needs to be done for the strategy to be effective.

Data Protection Champions

Data Protection Champions are members of staff in each team who support the IAO to promote good practices on information handling and provide support to other staff with regards to compliance with UK GDPR/DPA 2018.

Direction

In line with our governance structure, overall direction for compliance with and adherence to the UK GDPR/DPA 2018 is led from the top by the SLT in consultation with the Corporation. From the over-arching vision to decisions on processes, evidences, etc. there is direction at every level and for every task or activity to ensure our fulfilment of the UK GDPR/DPA 2018.

Reporting

We have a reporting structure that goes upwards from the bottom to the top ensuring accountability and ownership of tasks and activities that have been delegated to people at every level of the framework. Our accountability ensures that we are delivering on our commitment to keep personally identifiable information of our data subjects safe and secure.

Lawfulness of Processing - Consent

The College will use Consent as the primary lawful basis to collect, process, retain and dispose of personally identifiable information. This will be supported by other lawful basis in those contexts or situation where it may not be possible to obtain consent.

Security of Personal Data

We believe that security is key to any effective data protection programme or regime. At SGMC, we approach security of personally identifiable information at three levels…

1. People – all employees/staff are responsible for ensuring that any personal data that the College holds and for which they are responsible, is kept securely.
2. Information Systems/Information Technologies – our systems and technologies that we use as a College are protected to ensure the security of personal data
3. Physical Security – is our protection of people, e.g. staff, students, visitors, etc., hardware, e.g. desktop computers, laptops, etc., software, the network and data from physical actions and events that could cause serious loss or damage to the College.

Data Subject Access Request
Under the UK GDPR/DPA 2018, upholding the right of data subject access plays a central role in complying with the law. It is the only the Right of Access that allows the data subject to exercise further rights such as rectification and erasure. Where there is a data subject access request, the College will deal with the request in line with the appropriate procedure given the category of data subject that is making the request, e.g. parent/guardian or student.

Data Protection Impact Assessment (DPIA)
The College will assess the impact that any data processing, especially when we introduce or are going to be using a new technology to process data considering the nature, scope, context and purposes of the processing, where such technology or processing is likely to result in a high risk to the rights and freedoms of data subjects.

Data Retention & Disposal
SGMC will not keep any personal data for any period longer than is necessary. Every team, e.g. HR, and College function, e.g. Safeguarding, shall declare and document their retention period of their data in the SGMC – Data Retention and Disposal Schedule. Each team is also equipped with a paper shredder to use to shred all confidential waste when the information is no longer needed or due for disposal and on an annual basis, each team will do a data retention and disposal housekeeping to review what data has passed their retention period and due for disposal. This annual exercise shall be led by the DPG under the guidance of the DPO and the disposal arranged by the Estates team.

Data Protection Compliance Records
SGMC will keep appropriate and relevant records of it's data protection compliance work. The records will include policies, procedures, records, such as the Record of Processing Activities (ROPA) which is also the SGMC – Integrated Information Asset Register (IIAR), forms, agreements, notices, etc. These records will primarily be the evidence of work undertaken by SGMC to comply with the UK GDPR and the Data Protection Act 2018. The records will be stored in two main locations…

1. On Premise – in our secure data centre with access controls firmly in place
2. On the Cloud – through a Cloud-based service purchased for this purpose. The service is delivered by GDPRSentry and can be accessed via the link… www.gdprsentry.com. Access to records held in this Cloud-based data store is highly controlled through access credentials issued by the System Administrator, the DPO, and access to the records is also regulated based on the level of permission assigned to every user of the system.

It is intended that both the on-premise and the Cloud-based data stores will complement each other as the full repository of SGMC's data protection work records of evidence. However, on an annual basis, a backup of every record held in the Cloud-based system will be taken and stored safely in a separate but matching data store in the on-premise data centre.

Document Owner and Approval

The Data Protection Officer / UK GDPR Owner is the owner of this document and is responsible for ensuring that this policy framework document is reviewed annually.

A current version of this document is available to all members of staff on the Dashboard.

This policy framework document was approved by the Senior Leadership Team on 20th January 2021 and is issued on a version-controlled basis under the signature of the Senior Leadership Team.

Signature: David Ball Date: 20/01/2021

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	David Ball	11/02/2019
1.1	Review	David Ball	10/02/2020
2.0	Major Review	David Ball	20/01/2021
2.1	Review	David Ball	10/02/2022