Data Protection Policy

1. Intent

The intent of this policy is to establish an effective, accountable and transparent framework for ensuring compliance with the requirements of the EU General Data Protection Regulation 2016/679 (GDPR).

The GDPR sets out very severe sanctions (up to EUR 20,000,000) in the event of non-compliance, in addition to potential damage to the reputation of the School. Non-compliance is not an option.

2. Scope

This policy applies to all St George's staff (that is employees, trainees, interns, detached personnel, external music teachers, supply staff and temporary workers) and all third-party processors involved in the processing of personal data on behalf of St George's.

This policy does not apply to St George's staff's own personal/private files they store on St George's IT systems, provided they do not contain any personal data relating to the School.

3. Principles

St George's is committed to maintaining a high standard of education in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

Those who are involved in the processing of personal data must follow this policy. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action.

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, students, staff).

Key data protection terms used in this policy are:

- **Data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of students' personal information. As a data controller, we are responsible for safeguarding the use of personal data and compliance with GDPR.

- **Data processor** – an organisation that processes personal data on behalf of the School, for example a payroll provider or supplier of cloud-based software.

- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Personal information** (or **personal data**): any information relating to a living individual (a data subject), including name, identification number, photograph, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it can include expressions of opinion about the individual or any indication of someone's intentions towards that individual.

- **Processing** – anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

In case of doubt and generally before taking any action, reference should be made to the legal definitions of the above terms in the GDPR.

4. Data Protection Lead

The School has appointed the Finance and Administration Manager as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR.

5. Data Protection Coordinators

The school has appointed Data Protection Coordinator(s) to support the Data Protection Lead. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.
In case of questions and generally before taking any action concerning personal data (such as, starting a new processing or creating lists of students, families or

employees, disclosing personal data to third parties), St George's staff must consult the Data Protection Coordinator(s) to make sure that (1) the proposed action or processing complies with the GDPR, and (2) the latter can document such action or processing as required under the GDPR.

6. Requirements of the GDPR

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by the School (and any data processors it has contracted). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's 'accountability' principle also requires that the School not only process personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping a Data Map which lists our data processing activities;
- documenting significant decisions and assessments about how we use personal data; and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

7. Lawful grounds for data processing

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by St George's to provide school reports, medical care while on site, or document their educational progress. However, it will not be within their reasonable expectations that St George's would distribute data to third parties, share this data with other contacts, or publish it.

St George's will not process personal data or distribute it to a data processor unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes: consent should be used only if no other legal basis (as listed above) applies and/or if required by law;
- Processing is necessary for contractual necessity, e.g. to perform a contract with staff or parents, or pre-contractual measures with prospective students or employees;
- Processing is necessary for compliance with a legal obligation to which the School is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the School;
- Processing is necessary for the purposes of the legitimate interests pursued by the School or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child);
- Processing is necessary for compliance with a legal obligation, including in connection with employment and diversity;
- Processing is necessary under a narrower set of grounds for special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

8. Main responsibilities of staff

Record keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *their* personal data is inaccurate or untrue or if they are dissatisfied with the information in any way. Similarly, it is vital that personal data of others – in particular that of colleagues, students and their parents – is recorded accurately, professionally and appropriately.

Staff should take into consideration that the individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or students, in accordance with the School's other policies, and separate grounds may sometimes exist to withhold these from such requests. However, the

approach is to frame every document or email in such a way that you are able to stand by it if the subject person were to see it.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the Staff Handbook and all relevant School policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Acceptable Use of Computers
- Communications Policy
- Document Retention Policy
- IT e-Document Retention Policy
- IT e-Safety Policy
- IT Purchasing Policy
- IT Technical Security Policy
- Photographic and Video Images Policy
- Safer Recruitment Policy
- School Security Policy and Procedures
- Student Records Policy

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations is reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the CNPD (*Commission nationale pour la protection des données*) within 72 hours.

Common data breaches in the education sector include:

- Data sent by email to incorrect recipient
- Loss/theft of paperwork
- Cyber incidents
- Loss/ theft of unencrypted device
- Data posted or faxed to incorrect recipient
- Failure to redact data
- Errors in use of bcc when sending email
- Data left in insecure location

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. The School must keep a record of any personal data breaches, regardless of whether we need to notify the CNPD. If you become aware of a personal data breach, you must notify the Data Protection Coordinator(s) immediately at dataprotection@st-georges.lu. If staff are in any doubt as to whether they should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the staff member's contract.

Care and data security

More generally, we require all School staff to remain conscious of the data protection principles (see section 3 above), to attend any training required, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to reinforce these principles, to oversee the swift reporting of any concerns about how personal information is used by the School to the Data Protection Lead and to identity the need for (and implement) regular staff training.

9. Rights of Individuals / Subject Access Requests

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, or separate referral. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Data Protection Coordinator(s) as soon as possible and follow applicable procedures or guidelines as may be adopted by the School from time to time.

Subject to conditions, individuals also have the legal right to:

- require the School to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final point, none of these rights for individuals are absolute rights and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Data Protection Coordinator(s) as soon as possible.

10. Risk Assessment

Before introducing new technologies, new software, new information to be processed, or a new service, the School is obligated to carry out a Risk Assessment. Staff must complete a "New Apps/Software and IT Technology Requests" form online (available on the Staff Portal) and submit this to IT/Applications for review to assess if personal data is captured. If personal data is captured the Data Protection Coordinators will approve advise on GDPR requirements.

Please keep in mind that the use of new technology and the use of personal details is NOT permitted until the risk assessment has been completed and authorization has been provided.

It is crucial that the Data Protection Coordinator(s) be informed well in advance of any such project, as compliance with the GDPR may require significant work, verifications or formalities in certain instances. All forms must be submitted by the 1st May each year, so the Apps/Software and IT Technology lists are fully updated before parental consent can be obtained.

In some cases, for example where sensitive personal information will be processed or the data processing is likely to result in a high risk to individuals, a more thorough Data Protection Impact Assessment (DPIA) may be necessary in consultation with the CNPD. Adequate time and budget should be allocated for this process when planning the project.

11. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The School therefore does not allow staff to use portable storage devices such as USB thumb drives, SD cards and/or portable hard drives and rather encourages staff to use Office 365 for storing documents. Guidelines for how to use Office 365 and Teams for document storage are available on Staff Portal.

Use of personal email accounts or personal mobile phones for official School business is not permitted.

12. Summary

Data protection is a vital part of the School's commitment to safeguarding and quality of education. It is important for the School's reputation, moral obligation and financial interests that all personal information is handled fairly, lawfully, securely and responsibly.

When dealing with personal information, it is useful to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen as a set of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.