KINGSTON
GRAMMAR SCHOOL
FOUNDED 1561

DATA PROTECTION POLICY

1. BACKGROUND

Data protection is an important legal compliance area for KGS (the "School"). During the course of the School's activities it collects, stores and processes personal data (some of which is sensitive in nature) about staff, students, their parents, contractors and other third parties (in a manner more fully detailed in the School's Privacy Notices). The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

The way in which data is collected, stored and processed is more fully detailed in the School's Privacy Notices which should be read in conjunction with this Policy. Because the collection and storage of data arises in a number of areas of the School's operations, other School policies also overlap with this Policy, as detailed below.

The School has two Privacy Notices:

1. Staff and Governors;
2. Parents, students and all other members of the KGS community eg Alumni.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK **GDPR**"), and the Data Protection Act 2018 (the "**DPA 2018**"). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law in the UK and will typically look into individuals' complaints routinely and without cost and has various powers to take action for breaches of the law.

The School is registered with the ICO as a Data Controller and has the registration number Z7584041.

2. KEY RELEVANT DATA PROTECTION TERMS

Key data protection terms used in this Policy are:

Data controller – a person or body that determines the purpose and means of the processing of personal data and who is legally responsible for how it is used. For example, KGS (including by its governors) is a controller. An independent contractor who makes their own decisions is also, separately, likely to be a controller.

Data processor – an organisation that processes personal data on behalf of a controller, for example a payroll provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

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) by which that individual may be identified by the controller. This may include the individual's name or any other form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal data will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's or any person's intentions towards that individual.

Processing – virtually anything done with personal data, 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.

3. PERSON RESPONSIBLE FOR DATA PROTECTION AT THE SCHOOL

The School has appointed the Director of Finance and Operations (DFO) 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 applicable data protection legislation.

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, or by email to data@kgs.org.uk.

4. WHO DOES THIS POLICY APPLY TO, AND WHEN?

This Policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including current, past and prospective students; their parents/carers (referred to in this policy as "parents"); staff, alumni, governors, contractors, third parties and all other members of the KGS community).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as processors on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party controllers – which may range from other schools, to parents and appropriate authorities, to casual workers and volunteers –each party will need a lawful basis to process that personal data and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

5. OTHER RELEVANT SCHOOL POLICIES

This Policy is central to KGS' governance and is of relevance to many other School policies. All School policies should therefore be read in conjunction with this Policy.

Of particular relevance are:

Privacy Notice (staff and governors)
Privacy Notice (parents, students and all other members of the KGS community
Records Management Policy and Records Retention Schedule
Data Breach Response Procedure
Taking Using and Storing Images of Children Policy
Staff IT Acceptable Use Policy
Safeguarding & Child Protection Policy and Procedures
Online Safety Policy
Biometrics Policy
CCTV Policy
Recruitment, Selection, and Disclosure Policy and Procedure
Code of Conduct for Staff
Disciplinary Procedure
Whistleblowing Procedure
Grievance Procedure
Anti-Bribery Policy
Student AI Policy
Staff AI Policy

6. KEY DATA PROTECTION PRINCIPLES

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

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

The UK GDPR's broader 'accountability' principle also requires that KGS not only processes 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 records of our data processing activities, by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); 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; when staff training was undertaken; how and when data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom) etc.

7. LAWFUL GROUNDS FOR DATA PROCESSING

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under UK GDPR (and the fact that consent can be withdrawn by the data subject), it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests.

The School's legitimate interests are set out in its Privacy Notices as the UK GDPR requires.

Other lawful grounds for data processing include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors; and
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

8. 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 *any* personal data is inaccurate or untrue or if they are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, students and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This right to request information must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or students and parents, in accordance with the School's

other policies. In some instances, there may be grounds to withhold such records from access requests. However, the starting position for staff is to record every document or email in a form they would be able to stand by should the person about whom it was recorded ask to see it.

9. DATA HANDLING AND INTERACTION WITH OTHER POLICIES

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 all relevant School policies and procedures, including those listed in paragraph 5 above. 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 policies in paragraph 5.

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

10. AVOIDING, MITIGATING AND REPORTING DATA BREACHES

One of the key obligations contained in the UK GDPR is to report personal data breaches. Staff should comply with the School's Data Breach Response Procedure.

Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within **72 hours.**

In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether the School is obliged to notify the ICO. In line with this requirement, if staff become aware of a personal data breach you must notify the DFO as Data Protection Lead. If staff are in any doubt as to whether or not to report any actual or potential breach internally, 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 be aware of them in order to make a decision as to next steps.

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 applicable staff member's contract.

11. CARE AND DATA SECURITY

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see above), to attend relevant training as 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 affects daily processes including filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery of information is, and what the consequences would be of loss or unauthorised access to it.

We expect all those with management / leadership responsibilities to be particular champions of these principles and 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.

12. USE OF THIRD PARTY PLATFORMS/SUPPLIERS

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the DFO in the first instance, and at as early a stage as possible.

13. AN INDIVIDUAL'S LEGAL RIGHTS INCLUDING SUBJECT ACCESS REQUESTS

In addition to the School's responsibilities when processing data, individuals have certain specific rights, including that of access to their personal data held by a controller (ie the School). This is known as the "subject access right" or the right to make "subject access requests".

The School will deal with subject access requests promptly, acknowledging that there is no requirement for a subject access request to be made formally nor for any individual making such a request to refer to the underlying legislation. If staff become aware of a subject access request (or indeed any communication from an individual about their personal data), they must inform the Data Protection Lead (the DFO) as soon as possible to allow the request to be dealt with promptly. Further information is available in the Privacy Notice.

Individuals also have legal rights to:

- require us to correct personal data that 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; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels that the processing activity has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply.

However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (ie where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw their consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on their consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, staff must inform the Data Protection Lead as soon as they are aware of any request from an individual who is or may be purporting to exercise one or more of their data protection rights.

14. 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. Staff should be conscious of these requirements when reading and applying other School's policies, as set out at 5 above. As such:

- Staff are not permitted to remove personal data in electronic form from the KGS digital environment (or to remove personal data in paper form from the School premises), without prior consent of the Data Protection Lead or member of the Executive;
- Where a staff member is permitted to access or take data offsite it must be handled, used and stored in a secure manner;
- Staff must not provide personal data of students or parents to third parties, including a volunteer or contractors, unless there is a lawful reason to do so;
- Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

Staff should be mindful of the increased data security risks associated with remote working which is now recognized as a more common practice.

15. PROCESSING OF FINANCIAL / CREDIT CARD DATA

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, seek further guidance from the Data Protection Lead (DFO).

Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

16. CONCLUSION

We all care about our own personal data so it is in everyone's interests to get data protection right and to think carefully about data protection issues. This means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is 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 feel comfortable with 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 not seen as oppressive red tape, or a reason not to do something necessary or important, but a code 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.

17. QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the Data Protection Lead:

Email: data@kgs.org.uk

The Director of Finance and Operations
Kingston Grammar School
70 London Road
Kingston upon Thames
Surrey
KT2 6PY