SIR THOMAS RICH'S
Draft Data Protection Policy

This policy in drafted in accordance with the requirements of the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 (DPA 2018).

Date reviewed: 25 May 2018 (subject to approval from Governors)
Next review date: 25 May 2020

Status: Statutory
Responsibility: The Governors have overall responsibility for compliance with the GDPR and the DPA 2018. The Headmaster is responsible for ensuring compliance with the policy and for ensuring that appropriate training is provided for staff. The Data Protection Lead (currently Mr D. Dempsey) manages the implementation of the policy within the day-to-day activities of the School and will seek advice from the Date Protection Officer (DPO) on compliance issues. The DPO is currently the contracted representative provided by GCC Services. It is a professional duty of all members of staff to ensure that they comply with this policy.

Contents:

1. Policy Statement

Everyone has rights with regard to the way in which their *personal data* is handled. During the course of our activities as an Academy we will collect, store and *process personal data* about our pupils, *workforce*, parents and others. This makes us a *data controller* in relation to that *personal data*.

The School is committed to the protection of all *personal data* and *Special Category Personal Data* for which we are the *data controller*.

The law imposes significant fines for failing to lawfully *process* and safeguard *personal data* and failure to comply with this policy may result in those fines being applied.

All members of our *workforce* must comply with this policy when *processing personal data* on our behalf. Any breach of this policy may result in disciplinary or other action.

All defined terms in this policy are indicated in italic text, and a list of definitions is included in the Annex to this policy.

2. The School's Commitments

The types of *personal data* that we may be required to handle include information about pupils, parents, our *workforce*, and others that we deal with. The *personal data* which we hold is subject to certain legal safeguards specified in the General *Data* Protection Regulation ('*GDPR*'), the [*Data* Protection Act 2018], and other regulations (together '*Data* Protection Legislation').

This policy and any other documents referred to in it set out the basis on which we will *process* any *personal data* we collect from *Data Subjects*, or that is provided to us by *Data Subjects* or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on *data* protection and the legal conditions that must be satisfied when we *process* personal *data*.

3. *Data* Protection Officer and *Data* Protection Lead

As an Academy we are required to appoint a *Data* Protection Officer (DPO) who is responsible for ensuring the school's compliance with the *Data* Protection Legislation. We have also appointed Gloucestershire County Council as our *Data* Protection Officer and they can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk.

In addition to this we have a *Data* Protection Lead (DPL) who is a member of the Senior Management Team with day-to-day responsibility for *Data* Protection – this is currently Mr D Dempsey (Assistant Headteacher) – dd@strs.org.uk. However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

4. *Data* Protection Principles

Anyone *processing personal data* must comply with the *data* protection principles. These provide that *personal data* must be:

- *processed* fairly and lawfully and transparently in relation to the *data subject*
- *processed* for specified, lawful purposes and in a way which is not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date
- not kept for any longer than is necessary for the purpose
- *processed* securely using appropriate technical and organisational measures.

Personal data must also:

- be *processed* in line with *Data Subjects*' rights
- not be transferred to people or organisations situated in other countries without adequate protection

We will comply with these principles in relation to any *processing* of *personal data* by the School.

5. Fair and lawful *processing*

Data Protection Legislation is not intended to prevent the *processing* of personal *data*, but to ensure that it is done fairly and without adversely affecting the rights of the *data* subject.

For *personal data* to be *processed* fairly, *Data Subjects* must be made aware:

- that the *personal data* is being *processed*
- why the *personal data* is being *processed*
- what the lawful basis is for that *processing* (see below)
- whether the *personal data* will be shared, and if so with whom
- the period for which the *personal data* will be held
- the existence of the *Data Subject's* rights in relation to the *processing* of that personal *data*

- the right of the *data* subject to raise a complaint with the Information Commissioner's Office in relation to any *processing*.

5.1 The Legal Grounds for *Data Processing*

For *personal data* to be *process*ed lawfully, it must be *process*ed on the basis of one of the legal grounds set out in the *Data* Protection Legislation. We will normally *process personal data* under the following legal grounds:

- **Contract:** where the *processing* is necessary for the performance of a contract between us and the *data* subject, such as an employment contract
- **Legal obligation:** the *processing* is necessary for the school to comply with the law (not including contractual obligations)
- **Consent:** where none of the above apply then we will seek the consent of the *data* subject to the *processing* of their personal *data*.

5.2 *Special Category Personal Data*

When *Special Category Personal Data* is being *process*ed then an additional legal ground must apply to that *processing*. We will normally only *process Special Category Personal Data* under following legal grounds:

- **Employment law:** where the *processing* is necessary for employment law purposes, for example in relation to sickness absence
- **Substantial public interest:** where the *processing* is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment
- **Health:** where the *processing* is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities
- **Consent:** where none of the above apply then we will seek the consent of the *data* subject to the *processing* of their *Special Category Personal Data*.

We will inform *Data Subjects* of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the *data* or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

If any *data* user is in doubt as to whether they can use any *personal data* for any purpose then they must contact the DPO before doing so.

5.3 Vital Interests

There may be circumstances where it is considered necessary to *process personal data* or *Special Category Personal Data* in order to protect the vital interests of a *data* subject. This might include medical emergencies where the *data* subject is not in a position to give consent to the *processing*. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

5.4 Consent

Where none of the other bases for *processing* set out above apply then the school must seek the consent of the *data* subject before *processing* any *personal data* for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from *Data Subjects*. When pupils and/or our *workforce* join the School a consent form will be required to be completed in relation to them.

We consider all of our pupils capable of understanding the consent being given and we therefore ask for consent jointly form both parents and pupils.

Where consent is required for any other *processing* of *personal data* of any *data* subject we will ensure that we:

- inform the *data* subject of exactly what we intend to do with their personal *data*
- require them to positively confirm that they consent
- inform the *data* subject of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a *data* subject giving their consent.

A record must always be kept of any consent, including how it was obtained and when.

6. *Processing* for limited purposes

In the course of our activities as a school, we may collect and *process* the *personal data* set out in our Schedule of *Processing* Activities. This may include *personal data* we receive directly from a *data* subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and *personal data* we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our *workforce*).

We will only *process personal data* for the specific purposes set out in our Schedule of *Processing* Activities or for any other purposes specifically permitted by *Data* Protection Legislation or for which specific consent has been provided by the *data* subject.

We will only collect *personal data* to the extent that it is required for the specific purpose notified to the *data* subject, unless otherwise permitted by *Data* Protection Legislation.

7. Notifying *Data Subjects*

If we collect *personal data* directly from *Data Subjects*, we will inform them about:

- our identity and contact details as *data controller* and those of the DPO
- the purpose or purposes and legal basis for which we intend to *process* that personal *data*
- the types of third parties, if any, with which we will share or to which we will disclose that personal *data*
- whether the *personal data* will be transferred outside the European Economic Area (EEA) and if so the safeguards in place
- the period for which their *personal data* will be stored, by reference to our Retention and Destruction Policy
- the existence of any automated decision making in the *processing* of the *personal data* along with the significance and envisaged consequences of the *processing* and the right to object to such decision making
- the rights of the *data* subject to object to or limit *processing*, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed *Data Subjects* that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive *personal data* about a *data* subject from other sources, we will provide the *data* subject with the above information as soon as possible thereafter, informing them of where the *personal data* was obtained from.

8. *Processing Data*

8.1 Adequate, relevant and non-excessive *processing*

We will only collect *personal data* to the extent that it is required for the specific purpose notified to the *data* subject, unless otherwise permitted by *Data* Protection Legislation.

8.2 Accurate *data*

We will ensure that *personal data* we hold is accurate and kept up to date. We will take reasonable steps to destroy or amend inaccurate or out-of-date *data*. *Data Subjects* have a right to have any inaccurate *personal data* rectified.

8.3 Timely *Processing*

We will not keep *personal data* longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all *personal data* which is no longer required.

9. *Processing* in Line With the *Data Subject's* Rights

We will *process* all *personal data* in line with *Data Subjects*' rights, in particular their right to:

- request access to any *personal data* we hold about them
- object to the *processing* of their personal *data*, including the right to object to direct marketing
- have inaccurate or incomplete *personal data* about them rectified
- restrict *processing* of their *personal data*
- have *personal data* we hold about them erased
- have their *personal data* transferred
- object to the making of decisions about them by automated means.

9.1 The Right of Access to *Personal data* – Subject Access Requests

Data Subjects may request access to all *personal data* we hold about them. We shall respond to such requests within one month and they should be made in writing to:

Mr Matthew Morgan
Sir Thomas Rich's School
Oakleaze
Gloucester
GL2 0LF

No charge will be applied to *process* the request.

9.2 The Right to Object

In certain circumstances *Data Subjects* may object to us *processing* their personal *data*. This right may be exercised in relation to *processing* that we are undertaking on a basis other than consent.
An objection to *processing* does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the *data* subject. Such considerations are complex and will be referred to the DPO upon receipt of the request to exercise this right.

9.3 The Right to Rectification

If a *data* subject informs the School that *personal data* held about them by the School is inaccurate or incomplete then we will consider that request and provide a response in accordance with the legally set out timeframes (usually one month).

9.4 The Right to be Forgotten

Data Subjects have a right to have *personal data* about them held by the School erased only in the following circumstances:

- Where the *personal data* is no longer necessary for the purpose for which it was originally collected.
- When a *data* subject withdraws consent – which will apply only where the School is relying on the individuals consent to the *processing* in the first place.
- When a *data* subject objects to the *processing* and there is no overriding legitimate interest to continue that *processing* – see above in relation to the right to object.
- Where the *processing* of the *personal data* is otherwise unlawful.
- When it is necessary to erase the *personal data* to comply with a legal obligation.

The School does not have to comply with such requests if *processing* is taking place:

- to exercise the right of freedom of expression or information
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
- for public health purposes in the public interest
- for archiving purposes in the public interest, research or statistical purposes
- in relation to a legal claim.

If the School has shared the relevant *personal data* with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.
The DPO will be consulted in relation to requests under this right.

9.5 The Right to *Data* Portability

In limited circumstances a *data* subject has a right to receive their *personal data* in a machine readable format, and to have this transferred to other organisation. If such a request is made then the DPO will be consulted.

10. *Data* Security

We will take appropriate security measures against unlawful or unauthorised *processing* of personal *data*, and against the accidental loss of, or damage to, personal *data*.

We will put in place procedures and technologies to maintain the security of all *personal data* from the point of collection to the point of destruction.

Security procedures include:

- **Entry controls**: Site Security should be maintained in accordance with the School's Safeguarding Policy
- **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal:** Paper documents containing *personal data* should be disposed of using the Confidential Paper Waste bins provided. Digital storage devices should be given to the ICT department to be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
- **Equipment:** *Data* users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Taking paper documents away from school:** Any staff taking paper documents containing *personal data* away from the school site should take the appropriate degree of care with such documents to ensure their security. They should be returned to school as soon as is possible and any losses should be reported to the school immediately.
- **Working remotely or on your own device:** See the Staff Personal Device Policy (Part of the School's ICT Policy). USB storage devices, other than those authorised and encrypted by the school, will be disabled on school machines. Such devices will only be permitted where necessary.
- **Document printing:** Documents containing *personal data* must be collected immediately from printers and not left on photocopiers. The school has implemented a biometric retrieval *process* on some printers to help ensure this.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

11. *Data* Protection Impact Assessments

The School takes *data* protection very seriously, and will consider and comply with the requirements of *Data* Protection Legislation in relation to all of its activities whenever these involve the use of personal *data*, in accordance with the principles of *data* protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed *processing*. This includes where we intend to use new technologies which might pose a high risk to the rights of *Data Subjects* because of the types of *data* we will be *processing* or the way that we intend to do so.
The School will complete an assessment of any such proposed *processing*.

12. Disclosure and sharing of personal information

We may share *personal data* that we hold about *Data Subjects*, and without their consent, with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

The School will inform *Data Subjects* of any sharing of their *personal data* unless we are not legally required to do so, for example where *personal data* is shared with the police in the investigation of a criminal offence. In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

13. *Data Processors*

We contract with various organisations that provide services to the School, including:
Tucasi (online payments), EPM (personnel services), Show My Homework, Microsoft (email hosting), curriculum resource providers (e.g. MyMaths)

In order that these services can be provided effectively we are required to transfer *personal data* of *Data Subjects* to these *Data Processors*. *Personal data* will only be transferred to a *data processo*r if they agree to comply with our procedures and policies in relation to *data* security, or if they put in place adequate measures themselves to the satisfaction of the School The School will always undertake due diligence of any *data processo*r before transferring the *personal data* of *Data Subjects* to them.

Contracts with *Data Processors* will comply with *Data* Protection Legislation and contain explicit obligations on the *data processo*r to ensure compliance with the *Data* Protection Legislation, and compliance with the rights of *Data Subjects*.

14. Images, videos and CCTV

Parents and others attending School events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The School does not prohibit this as a matter of policy.

The School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the School to prevent. The School asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

As a School we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

Whenever a pupil begins their attendance at the School, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will use images of pupils for the means of identification within school but we will not use images or videos of pupils for any other purpose where we do not have consent.

The School operates a CCTV system. Please refer to the School's CCTV Policy (part of the ICT Policy).

15. *Data* Retention and Disposal

Data will be retained in accordance with our *Data* Retention and Deletion Schedule.

16. Complaints

A complaint by an individual about the way in which the School handles *data* protection should be directed to the ICO. https://ico.org.uk. Helpline: 0303 1231113 or 01625 545745. If it considers the complaint legitimate, it may ask the School to take steps to comply with the DPA or serve an enforcement notice.

The requester may apply for a court order compelling the School to comply. It is a matter for the courts to decide whether to make such an order.

If an individual suffers damage because the school has breached the DPA he/she is entitled to compensation from the School. This can only be enforced through the courts.

Appendix A

Schedule 2 Conditions

Unless a relevant exemption applies, at least one of the following conditions must be met whenever the School *processes* personal *data*:

- The individual who the *personal data* is about has consented to the *processing*.
- The *processing* is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The *processing* is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The *processing* is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The *processing* is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The *processing* is in accordance with the "legitimate interests" condition.

Schedule 3 Conditions

If the information is sensitive personal *data*, at least one of several other conditions must also be met before the *processing* can comply with the first *data* protection principle. These other conditions are as follows:

- The individual who the sensitive *personal data* is about has given explicit consent to the *processing*.
- The *processing* is necessary so that you can comply with employment law.
- The *processing* is necessary to protect the vital interests of:
  - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual's consent has been unreasonably withheld).
- The *processing* is carried out by a not-for-profit organisation and does not involve disclosing *personal data* to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The *processing* is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The *processing* is necessary for administering justice, or for exercising statutory or governmental functions.
- The *processing* is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.

- The *processing* is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for *processing* sensitive personal *data*. Their effect is to permit the *processing* of sensitive *personal data* for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for *processing* is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

ANNEX

DEFINITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal *data*. This includes pupils, our workforce, staff, and other individuals. A *data* subject need not be a UK national or resident. All *Data Subjects* have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable natural person (a *data* subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location *data*, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal *data* is processed. They are responsible for establishing practices and policies in line with *Data Protection Legislation*. We are the *data* controller of all personal *data* used in our business for our own commercial purposes.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal *data*. *Data* users must protect the *data* they handle in accordance with this *data* protection policy and any applicable *data* security procedures at all times.
Data Processors	Any person or organisation that is not a *data* user that processes personal *data* on our behalf and on our instructions.
Processing	Any activity that involves use of the *data*. It includes obtaining, recording or holding the *data*, or carrying out any operation or set of operations on the *data* such as 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. Processing also includes transferring personal *data* to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric *data*.
Workforce	Includes any individual employed by the School such as staff and those who volunteer in any capacity including governors and parent helpers.