DATA PROTECTION POLICY

This policy applies to all schools within the Royal Russell Trust Group of Schools and all members of staff and pupils, whether permanent, temporary, casual, part-time or on fixed-term contracts, volunteers and to job applicants.

Background

Data protection is an important legal compliance issue for Russell School Trust. During the Trust's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the Trust's Privacy Policy).

The Trust, 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 Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) controls how your personal information is used. Information on the Data Protection Act 2018 can be found here.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, will typically investigate individuals' complaints routinely and without cost, and has various powers to act for breaches of the law.

Definitions

Key data protection terms used in this data protection 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, the Trust (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller

- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT 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. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information 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 Trust's, or any person's, intentions towards that individual

- **Processing** – virtually 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

Application of this policy

This policy sets out the Trust's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, past pupils and their parents, applicants, employees, contractors and third parties).

Those who handle personal data as employees or governors of the Trust 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 Trust or individuals will be considered a serious matter.

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

Where the Trust shares personal data with third party data controllers, which may range from other schools, to parents, to 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.

Volunteers and contractors to the Trust can also be data controllers, and the same legal regime and best practice standards set out in this policy will apply to them in law.

Person responsible for Data Protection

The Trust has appointed the Director of Operations and Finance as the Data Protection Officer who will endeavour to ensure that all personal data is processed in compliance with this Policy and 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 Operations Manager, who is the nominated Data Protection Co-ordinator.

The Principles

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

1. Processed **lawfully, fairly** and in a **transparent** manner

2. Collected for **specific, explicit and legitimate purposes** and only for the purposes it was collected for

3. **Adequate, relevant** and **limited** to what is necessary for the purposes for which 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 processed in a manner that ensures **appropriate security** of the personal data.

6. The broader 'accountability' principle also requires that the Trust 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, including by way of logs and policies
   - documenting significant decisions and assessments about how we use personal data (including via formal risk assessments 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 any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc

7. The data controller shall be responsible for and be able to demonstrate compliance with all of the above principles.

Lawful grounds for data processing

There are 6 different lawful grounds for processing personal data: consent, contract, legal obligation, vital interests, public task and legitimate interests. However, because the definition of what constitutes consent is relatively strict (and can be withdrawn by the data subject) it is considered preferable for the Trust 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 Trust. It can be challenged by data subjects and also means the Trust is taking on extra responsibility for considering and protecting people's rights and interests. The Trust's legitimate interests are set out in its Privacy Notice.

Other likely lawful grounds 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
- 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

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the Trust is accurate, fair and adequate. Staff are required to inform the Trust if they believe that *any* personal data is inaccurate or untrue or if you 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, pupils and their parents, in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individual(s) about whom they record information on Trust business, notably in emails and notes, digitally or in hard copy files, 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 pupils, in accordance with the Trust's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a**

form they would be prepared to stand by should the person about whom it was recorded ask to see it.

Data Handling

All staff have a responsibility to handle the personal data which they encounter fairly, lawfully, responsibly and securely and in accordance with the law and all relevant Trust policies and procedures (to the extent applicable to them). There are data protection implications across several areas of the Trust's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Safeguarding Policy
- ICT Acceptable Use Policy (Due for review September 2025)
- Data Retention Policy (Due for review September 2025)
- Privacy Policy (Due for review September 2025)
- Online Safety Policy Due for review January 2026)

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 obligation is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data 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 Trust must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach, they must notify the Data Protection Officer. If staff are in any doubt as to whether to report something 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 Trust always needs to know about them to decide.

As stated above, the Trust may not need to treat the incident itself as a disciplinary matter, however a failure to report could result in significant exposure for the Trust, 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 Trust staff (and expect all our contractors) to remain mindful of the data protection principles, 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: filing and sending correspondence, notably hard copy documents. Data handlers 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 be champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the Trust to the Data Protection Co-ordinator, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Rights of Individuals

In addition to the Trust's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the Trust). 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, nor to refer to the correct legislation. 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 Officer as soon as possible, either verbally or in writing.

Individuals also have legal rights to:

- require us 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 situation, to any of our processing activities where the individual feels this has a disproportionate impact on them; and 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 (i.e. where a significant decision is made about the individual without human intervention)
    - object to direct marketing; and
    - withdraw one's 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 consent, or of any processing carried out on some other legal basis other than consent)

In any event, 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 Officer as soon as possible.

Data Security: online and digital

The Trust 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 in accordance with the ICT Acceptable Use Policies.

Processing of Financial/Credit Card Data

The Trust complies with the requirements of the Payment Card Industry 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, please seek further guidance from the Director of Operations and Finance. 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.

Data Protection Policy – Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information the Trust will hold and how it will be held or used.

Data Subject – The living individual whom the Trust will collect, hold and process their personal data on behalf of.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Explicit consent – is a freely given, specific and informed agreement by a Data Subject in the processing of personal information about her/him. Explicit consent is needed for processing sensitive personal data.

Notification – Notifying the Information Commissioner about the data processing activities of the Trust as certain activities may be exempt from notification.

This link will take you to the ICO website where a self-assessment guide will help you to decide if you are exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified, e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees.

Sensitive personal data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

UK General Protection Regulation (UK GDPR) – the general data protection regime that applies to most UK businesses and organisations, tailored by the Data Protection Act 2018.

Approved by		
Reviewed regularly	from	May 2022
Reviewed and approved by	SLT	April 2023
Reviewed and approved by	F&E	May 2023
Reviewed and approved by	Board	June 2023
Reviewed and approved by	F&E	May 2024
Reviewed and approved by	Board	June 2024
Reviewed and approved by	F&E	June 2025
Reviewed and approved by	Board	June 2025
Reviewed	Mr Cufley/Mr Cobill	October 2025
Reviewed and approved by	F&E	November 2025
Reviewed and approved by	Board	December 2025
Next review due		September 2026