

**DATA PROTECTION POLICY**  
2024-2025

Contents

1. Policy Statement.....	2
2. Application Guidance.....	2
2.1 What is "personal data", who is covered, and what is meant by "processing" personal data?.....	2
2.2 Data Subjects - Meaning of "students", "parents", and "Staff" .....	3
2.3 College Staff nominated to monitor Data Protection.....	3
2.4 Processing of personal data by the college (Students and Parents/Guardians data).....	4
2.5 Processing of personal data by the college (Staff data).....	4
2.6 Processing of personal data by RGSW (General data).....	5
2.7 Sensitive personal data.....	5
3. Rights of access to personal data (Subject Access Request).....	6
3.1 Who can exercise rights?.....	7
3.2 Requests from third parties concerning disclosure of personal data.....	7
4. Publication of personal data.....	7
4.1 Third parties with whom the college may need to share your personal data.....	8
4.2 Transferring Personal Data to a Country Outside the EEA.....	8
5. Responsibilities and obligations of staff members and governors of the college.....	9
5.1 Staff Photographs.....	9
5.2 Accuracy of personal data held by college.....	9
5.3 Third Party Data Processors.....	9
Appendix 1.....	10



## 1. Policy Statement

This policy applies to Rochester Independent College ("the college").

The college is registered under the UK Data Protection Act 1998 ("the DPA"), and is compliant with General Data Protection Regulation ("GDPR").

It is the specific policy of the college to:-

- take all appropriate and reasonable steps to ensure the rights of the college staff, students, parents and governors ("Data Subjects"), with respect to their personal data, are protected;
- to take all reasonable steps to ensure that personal data held by the college in relation to a Data Subject is both accurate and secure; and to comply with the DPA and GDPR

All members of college staff will be made aware of this policy and of their duties under the DPA and GDPR. This policy will be published both externally as well as internally.

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.

## 2. Application Guidance

The college is required to process relevant personal data regarding staff members, students and their parents and guardians as part of the conduct of its day-to-day operations.

This policy, which includes the application guidance set out below, details how the college will ensure compliance with its obligations with respect to the protection of personal data that it holds and uses.

### 2.1 What is "personal data", who is covered, and what is meant by "processing" personal data?

"Personal data" means any information relating to an identified or identifiable natural person.

"Identifiable" in this context means one who can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to physical, physiological, mental, economic, cultural, or social identity.

Individuals meeting this definition may include current, past or prospective students, their families/guardians, and staff members or governors or other relevant Data Subjects.

It is important to note that personal data processed by the college in respect of staff, students and parents and guardians covers both facts and opinions about those individuals.

The processing of personal data may include obtaining, recording, holding, disclosing, destroying, or otherwise using that data.

Every school/college is required, as part of its operation, to process a wide range of personal data. Personal data may include, inter alia:-

- Names, addresses, dates of birth



- National Insurance numbers
- Bank details and other financial information
- Academic, disciplinary, admissions and attendance records and references
- Medical records
- Examination scripts and marks
- Photographs
- Video and CCTV images
- Biometrics (relating to student health and security)

For the purposes of the DPA, the college is the "data controller" of all personal data that is held about the Data Subject.

## 2.2 Data Subjects - Meaning of "students", "parents", and "Staff"

In the context of the scope of this policy any reference to "students" includes current, past or prospective students.

Any reference to "parents and guardians" includes the parents and guardians of current, past or prospective students.

Any reference to "staff" in the context of the scope of this policy may include visiting music or sports staff, contractors, agencies or self-employed individuals contracted by the school to provide a service including governors and some Dukes members of staff, or other employees with a specific, role-related requirement including cover teachers/agencies to view personal data, including sensitive personal data. Such a named individual will, at their legitimate request, be granted either 'read and write' or 'read only' access as appropriate to specified data by the Data Protection Controller ("DPC").

## 2.3 College Staff nominated to monitor Data Protection

The college staff who have been nominated to be our data champion and to monitor data protection issues is:-

Alistair Donaldson

The Principal will endeavour to ensure that all personal data at the college is processed in compliance with this policy and the principles of the DPA and GDPR.

The data champion will also provide education, training and support to staff, as well as police this policy to ensure that all applicable data at the college is processed in compliance with this policy. If an individual believes that any non-compliance with this policy has occurred they should notify the data champion and the Principal immediately. The ultimate responsibility for matters in this policy lies with the Principal.

## 2.4 Processing of personal data by the college (Students and Parents/Guardians data)

The college may process a wide range of personal data about students, their parents, or guardians as part of its operations. This personal data may include (but is not limited to):

- contact details
- National Curriculum and other assessment results
- attendance data
- disciplinary data
- admissions data
- references
- examination scripts and marks
- details relating to special educational needs
- images of pupils engaging in School activities

In relation to parents and/or guardians, personal data may include financial information.



The college may also process sensitive personal data such as ethnic group, religious beliefs, and relevant medical information.

Personal data will usually be collected directly from parents/pupils, but some may be passed to the School by third parties.

Student data (including sensitive personal data, where appropriate) is processed by the college strictly in accordance with the DPA and GDPR in order to:

- support its students' teaching and learning
- monitor and report on their progress
- publish examination results as separately notified to affected students and/or their parents and/or guardians
- provide appropriate pastoral care
- assess how well the college as a whole is doing
- communicate with former students
- monitor students' and staff members' email communications and internet-use to ensure compliance with the college policy on the 'use of college computers and internet access'
- where appropriate, promote the college to prospective students (including through the college's prospectus and online portals including intranets and websites and other promotional material)
- fulfil other reasonable purposes relating to the operation of the college.

Unless students, parents and/or guardians have requested otherwise, the college may also use their contact details to send them promotional and marketing information about the college by post, email, and SMS.

## 2.5 Processing of personal data by the college (Staff data)

As noted, personal data processed by the college in respect of staff members covers both facts and opinions about the individual concerned. It includes information necessary for employment such as the staff member's name, address, and details for payment of salary.

A staff member's consent may be required for the processing of personal data, unless processing is necessary for the performance of the contract of employment, without breaching the terms of the DPA or GDPR.

Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential, and will only be disclosed to third parties with the consent of the staff member.

## 2.6 Processing of personal data by RGSW (General data)

In accordance with the eight Data Protection Principles in the DPA, the college shall do all that is reasonable to ensure that all personal data is:

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than necessary
- Processed in accordance with the Data Subject's rights
- Secure
- Not transferred to other countries without adequate protection

We shall only process personal data about a student, a parent, a guardian, a staff member or governor if relevant consent has been given and/or the processing is necessary -

- For the performance of our contract with parents;  
or



- To comply with a legal obligation;  
or
- To protect the vital interests of the Data Subject;  
or
- For the administration of justice;  
or
- For the legitimate interests of the School or a third party (such as another school or an examining board).

## 2.7 Sensitive personal data

We may, from time to time, be required to process sensitive personal data relating to a student, a parent, a legal guardian, education guardian or staff member. Sensitive personal data is information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health or condition, sexual life, criminal offences and sentences imposed.

Sensitive personal data will generally be processed only where one of the following conditions applies: -

- The Data Subject has given explicit consent;  
or
- The information has already been made public by the Data Subject;  
or
- There is a medical or statutory requirement to process the data, for example, a statutory requirement to safeguard and promote the welfare of the Data Subject or any statutory requirement to notify a suspicion of money laundering, or co-operate with the authorities in other ways.

Such data will not be copied or shared with any third party other than with the express, written permission of the Data Protection nominated person. Provision of access will be restricted solely to data which is needed for the individual to fulfil their contract of service with the college properly and to the best of their ability, and does not contravene the terms of this policy, the Data Protection Act 1998 ("the Act") or the Computer Misuse Act.

## 3. Rights of access to personal data (Subject Access Request)

Individuals have a right of access to their own personal data unless an exemption applies (see below). An individual wishing to access their personal data held by the college should put their request in writing to the nominated person. The nominated person shall respond to a request for access to records within forty days of receiving the request (or earlier if practicable).

For these purposes, a request which arrives while the college is closed for holidays will be treated as having been received when the college next re-opens.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship the student if applicable.

Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

*This list is not exhaustive.*

The DPA provides that certain data is exempt from the right of access, including:-



Information which identifies other individuals.

Information which we reasonably believe likely to cause damage or distress.

- Data prepared solely or mainly to request or give legal advice.
- Examination scripts written by a pupil.
- Data that does not concern a living individual.
- Data that is not part of a manual or electronic filing system.
- Data that may be evidence in criminal proceedings.
- (In some cases) documents protected by copyright.

The college shall also treat as confidential any reference in the colleges' possession which has been prepared or given to UCAS and any reference for current or prospective education, training or employment of a student or staff member.

The college acknowledge that an individual may have a right of access to a reference which the college has received about them from another source. Such reference will only be disclosed, however, if:-

- Disclosure will not identify the source of the reference; or
- The referee has given consent; or
- Disclosure is reasonable in all the circumstances.

The college shall take reasonable steps to ensure that members of staff will only have access to personal data relating to students, their parents or guardians, or staff members where it is reasonably necessary for them to do so.

### 3.1 Who can exercise rights?

Rights under the DPA and GDPR belong to the individual to whom the personal data relates. In most cases, however, the college is entitled to rely on parental consent to process data relating to students unless, in the particular circumstances, it is unreasonable to rely on the parents' consent. This could arise, for example, if there is a conflict of interests between parents and a student or if disclosure of information would interfere with a student's lawful right to confidentiality. The college shall only grant a student direct access to their personal data if we reasonably believe that the student understands the nature of the request and that access would not be likely to cause damage or distress to the student or other students.

### 3.2 Requests from third parties concerning disclosure of personal data

The college will normally disclose such data as is necessary to third parties for the following purposes:-

- To give a confidential reference relating to a Data Subject to any educational institution which it is proposed that the student may attend, or to a prospective employer;
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that a student may attend;
- To publish the results of public examinations or other achievements of students at the college;
- To publish non-portrait-style photographs or images of students who are not identified by name in a college prospectus or promotional video or on an college website or online portal;
- To disclose details of a student's medical condition, allergies or disability, where it is in the student's interests that we do so, for example, for medical advice, insurance purposes or to staff members supervising sports and games or to organisers of trips, or third parties whom the college contracts to offer goods/services to college students, governors, parents or staff members.

In most other cases, the college shall not generally disclose personal data to third parties unless the Data Subject has given consent or one of the specific exemptions under the Act applies. If the college receives a disclosure request from a third party the colleges will take all reasonable steps to verify the identity of the third party before making any disclosure.



#### 4. Publication of personal data

A parent, or student aged 12 years plus, who wishes to limit or object to the student's image being used in the college's promotional material should notify the nominated persons in writing. In the absence of notification, the college shall, from time to time, make use of personal data relating to students, their parents or guardians in the following ways:-

- In the college prospectus, on a college website/online portal or in other promotional literature or materials; the college shall not, however, publish a portrait-style photograph or the student's name with the image identifying the student without the express agreement of a parent and the student.
- To compile and maintain a register of current or former students or any necessary list of students representing the college as a member of a team or on a college trip.
- To give information relating to the fundraising activities of the college and initiatives considered beneficial to members of the college community.
- To maintain contact with former members of the college and their association and to inform them of events and activities.

##### 4.1 Third parties with whom the college may need to share your personal data

From time to time the college may pass personal data (including sensitive personal data where appropriate) to third parties, including local authorities, other public authorities, independent school bodies such as the Independent Schools Inspectorate, and the Independent Schools Council, health professionals and the college's professional advisers, who will process the data:

- to enable the relevant authorities to monitor the colleges' performance;
- to compile statistical information (normally used on an anonymous basis);
- to safeguard students' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for students;
- where specifically requested by students and/or their parents or guardians;
- where necessary in connection with learning and co-curricular activities undertaken by students;
- to enable students to take part in national and other assessments and to monitor students' progress and educational needs;
- to obtain appropriate professional advice and insurance for the college;
- where a reference or other information about a student or ex-student is requested by another educational establishment or employer to whom they have applied;
- where otherwise required by law; and
- otherwise where reasonably necessary for the operation of the college.

The college may also, unless a data subject requests otherwise, share personal data about former students with any association, society or club set up to establish or maintain relationships with alumni of the college, who may contact alumni from time to time by post, email, social media and SMS about the college and its activities.

##### 4.2 Transferring Personal Data to a Country Outside the EEA

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.



- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.
- Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

## 5. Responsibilities and obligations of staff members and governors of the college

All staff members and governors of the college have a responsibility to ensure that they process any data in relation to a Data Subjects' files in accordance with this Data Protection Policy, and in particular to ensure that that it is adequate, relevant and not excessive and also accurate and up-to-date.

All staff members and governors must ensure that any data they need to access is kept secure, both while stored or in transit. Data moved via third party web/cloud based services should be encrypted.

Data that is the subject of this policy should not be stored outside the college IT systems unless express written authority has been given by the nominated person. Staff members must also not pass any home contact details (staff, student or parent) to other parties without the consent of the Data Subject, or parent/guardian of the Data Subject as applicable.

### 5.1 Staff Photographs

Staff Photographs will be used for security and safeguarding purposes internally within the college organisation, as well as for promotional purposes. Any staff member who wishes to limit their image being used in college promotional material should notify the Principal in writing.

### 5.2 Accuracy of personal data held by college

The college shall do all that is reasonable to ensure that personal data held in relation to an individual from time to time is accurate. Individuals must notify the nominated person of any changes to information held about them.

A Data Subject has the right to request that inaccurate information about them is erased or corrected.

### 5.3 Third Party Data Processors

Access to data may be granted to visiting teachers, contractors, agencies or self-employed individuals contracted by the college to provide a service, or other employees with a specific, role-related requirement including cover teachers/agencies to view personal data, including sensitive personal data. Where this is the case, the aforementioned individuals will be required to sign and return Appendix 1, having read this policy.

The college may appoint individuals not directly employed by the college to act on their behalf as Data Processors. This may include but is not limited to individuals, companies and organisations supplying, installing and/or maintaining Computing and IT systems and infrastructure. In these cases the levels of access, security and processing will be specified by the college as part of the contract and personal data cannot be used outside these terms.





If an individual believes that we have not complied with this policy or have acted otherwise than in accordance with the Act, they should notify the nominated person.

Created/Updated	Author	Approved by	Date
September 2017	PL	AB	September 2017
August 2018	AD	AB	August 2018
August 2019	AD	AB	August 2019
August 2020	AD	AB	August 2020
August 2021	AD	AB	August 2021
August 2022	AD	AB	August 2022
August 2023	AD	AB	August 2023
August 2024	AD	AB	August 2024

#### Appendix 1

##### ACCESS AGREEMENT BETWEEN VISITING STAFF/CONTRACTORS AND COLLEGE

(To be kept on staff HR files)

Access to data by visiting teachers, contractors, agencies or self-employed individuals contracted by the college to provide a service, or other employees with a specific, role-related requirement including cover teachers/agencies to view personal data, including sensitive personal data.

I the undersigned, have a legitimate reason to be granted 'read only' or 'read and write' access to personal data, which may include sensitive personal data held securely by the college.

I confirm my understanding of the college's Data Protection Policy, and undertake to abide by its conditions. In particular, my attention has been drawn to the obligation placed on me to adhere to the college Data Protection Policy, namely: Data shared, created or accessible by me/my organisation will not be copied or shared with any third party other than with the express, written permission of the college nominated person for data protection.

Provision of access will be restricted solely to data which is needed for the individual to fulfil their contract of service with the college properly and to the best of their ability, and does not contravene the terms of this policy or the Computer Misuse Act."

I also undertake to notify the nominated person(s) immediately in the following circumstances: -

- when I no longer have a legitimate need to access any or all of the data for which I have been granted access,
- 
- if I have reason to believe that my IT security has or may have been compromised in any way, thereby affecting the security of the college's data to which I have, or have had, access.

I understand that my access rights may be withdrawn at any time by the nominated person (s) who will notify me if this occurs.



Signed .....

Dated .....