

**CITY OF ROCHESTER SCHOOL  
DATA PROTECTION POLICY**

*This policy applies to the whole school and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office.*

**Monitoring and Review:**

- This policy will be subject to continuous monitoring, refinement and audit by the Headteacher, being responsible for the day to day organisation of the curriculum, monitoring the weekly lesson plans for all staff, ensuring all planning is appropriately differentiated with relevant, appropriate learning objectives.
- The Trustees undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so requires. This discussion will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay.

Signed:

Date Reviewed: September 2023  
Date of Next Review: September 2024  
Version No. 3



Alicja Emmett  
Headteacher



Kirstine Boon  
Chair of Trustees

This policy will be reviewed no later than September 2024, or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

The Designated Privacy and Compliance Officers of City of Rochester School are Kieran Yates and Michelle Homer who can be contacted on: [pco@cityofrochesterschool.org](mailto:pco@cityofrochesterschool.org)

**Contents**

1. Aims .....	2
2. Legislation and guidance .....	2
3. Definitions.....	2
4. The data controller .....	3
5. Roles and responsibilities .....	3
6. Data protection principles .....	3
7. Collecting personal data .....	4
8. Sharing personal data .....	4
9. Subject access requests and other rights of individuals.....	5
10. Parental requests to see the educational record .....	6
11. Photographs and videos .....	6
12. Data protection by design and default .....	6
13. Data security and storage of records .....	7
14. Disposal of records .....	7
15. Personal data breaches .....	7
16. Training .....	8
17. Monitoring arrangements .....	8

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

### 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

### 2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the [GDPR](#) and the ICO’s [code of practice for subject access requests](#). It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data. It also reflects the ICO’s [code of practice](#) for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child’s educational record.

### 3. Definitions

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual. This may include the individual’s: <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.
<b>Special categories of personal data</b>	Personal data which is more sensitive and so needs more protection, including information about an individual’s: <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>• Health – physical or mental</li><li>• Sex life or sexual orientation</li></ul>
<b>Processing</b>	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data. In our case this is in the person of our lead proprietor.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

#### 4. The Data Controller

City of Rochester School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. Following guidance on the ICO website, the school has not registered a Data Protection Officer with the ICO and instead has appointed a Privacy and Compliance Officer (PCO) in charge of processing data within the school.

#### 5. Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1. **The Trustee;** The Proprietor (magic (UK) Ltd) via the trustees has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. **Data Protection Officer:** In line with ICO guidance, there is not a Data Protection Officer (DPO) registered for City of Rochester School.

5.3. **Privacy and Compliance Officer:** The Privacy and Compliance Officer/s (PCO) is/are responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. In City of Rochester School the PCOs are Kieran Yates and Michelle Homer. The PCO will provide an annual report of their activities to the School Advisory Board in the summer term and, where relevant, report to the board their advice and recommendations on school data protection issues. The PCO is also the first point of contact for individuals whose data the school processes, and for the ICO.

5.4. **Headteacher:** The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.5. **All staff:** Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the PCO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach – see the City of Rochester School Data Breach Procedure
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

#### 6. Data Protection Principles

The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

## 7. Collecting Personal Data

### 7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public licensed body, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps which require use of personal data, and we intend to rely on consent as a basis for processing, we will get parental consent as some of our pupils are under 13.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

### 7.2 Limitation, minimisation and accuracy:

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

## 8. Sharing personal data:

We have a responsibility to share information with the local authority and Department for Education regarding educational results and concerns such as attendance and test results and within the scope of providing education for our pupils. We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## **9. Subject Access Requests and other rights of individuals**

### **9.1. Subject access requests:**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests will preferably be submitted in writing, either by letter or email to the PCO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the PCO, if this is not in writing the PCO will contact the requestee to verify the information that is required.

### **9.2. Children and subject access requests:**

Personal data about a child belongs to that child. However, as all of our children are aged 18 or below, apart from in exceptional circumstances, we would expect parents to act as owners of their children's data. Please see 9.1 above for subject access requests.

### **9.3. Responding to subject access requests:**

When responding to requests we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

#### **9.4. Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the PCO. If staff receive such a request, they must immediately forward it to the PCO.

#### **10. Parent Requests to see the Educational Records**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

#### **11. Photographs and Videos**

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/carer. Uses may include:

- Within school on notice boards, school posters, prospectus and newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, beyond the first name, where necessary to ensure they cannot be identified.

#### **12. Data Protection by design and default**

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified PCO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

to rights and freedoms of individuals, and when introducing new technologies (the PCO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and PCO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

### **13. Data Security and Storage of Records**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use or are password protected
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site it must be safeguarded, papers should be carried in locked bags or cases. The use by staff of removable media eg USB sticks is not permitted.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online safety policy and Acceptable use agreements)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

### **14. Disposal of Records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

### **15. Personal Data Breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches: In the unlikely event of a suspected data breach, we will follow the Data Breach Procedure attached to this Policy. When appropriate, we will report the data breach to the ICO within 72 hours. As example, breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing personal data about pupils

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

## **16. Training**

All staff and trustees are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## **17. Monitoring Arrangements**

The PCO is responsible for monitoring and reviewing this policy: This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the full trustee board



## Appendix 1:

### Personal data breach procedure:

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the PCO
- The PCO will investigate the report and determine whether a breach has occurred. To decide, the PCO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The PCO will alert the headteacher and the chair of trustees
- The PCO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The PCO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The PCO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the PCO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation
  - (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s)
  - concerned

If it's likely that there will be a risk to people's rights and freedoms, the PCO must notify the ICO.

- The PCO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school admin computer network, which is accessible by members of the admin team and the senior leadership team.
- Where the ICO must be notified, the PCO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the PCO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the PCO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

- If all the above details are not yet known, the PCO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the PCO expects to have further information. The PCO will submit the remaining information as soon as possible
- The PCO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the PCO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the PCO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The PCO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The PCO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school admin computer network, which is accessible by members of the admin team and the senior leadership team.

- The PCO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

**Actions to minimise the impact of data breaches:** We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

#### **Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the PCO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the PCO will ask the ICT suppliers (currently BDR) to recall it
- In any cases where the recall is unsuccessful, the PCO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The PCO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The PCO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

**Non-anonymised pupil exam results or staff pay information being shared with trustees**

- All paper documents recalled and shredded. If it is received by email, trustees must only access using their encrypted email and they will be asked to delete the info.
- The trustees confirm in writing that they have deleted the information.

**A device containing non-encrypted sensitive personal data being stolen or hacked**

- The incident will be reported to the police as soon as possible.
- If the device is a school registered device contact the school IT supplier (BDR) to wipe the device memory using appropriate software as soon as possible.
- If it is a personal device the member of staff must use their cloud supplier to wipe the device memory, they must confirm in writing that they have done this.
- Report to the PCO and assess what details could be accessible. The PCO will report to parents if suitable to the ICO.

## **Appendix 2:**

### **Privacy Notice (How we use pupil information)**

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)

This list is not exhaustive.

### **Why we collect and use pupil information**

We collect and use pupil information, for the following purposes:

- a) to support pupil learning
- b) to monitor and report on pupil attainment progress
- c) to provide appropriate pastoral care
- d) to assess the quality of our services
- e) to keep children safe (food allergies, or emergency contact details)
- f) to meet the statutory duties placed upon us for the Department for Education (DfE) data collections

### **Collecting pupil information**

We collect pupil information via Common Transfer Files, Registration documentation when joining the school, regularly updated questionnaires from parents/guardians such as medical questionnaires, EHCP and annual review documentation, CPOMS entries, conversations with parents/guardians via telephone, electronic methods such as email or face to face

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

### **Storing pupil data**

We hold pupil data securely for the set amount of time shown in our data retention schedule.

### **Who we share pupil information with**

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- social services
- attendance advisory

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

## Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

## Youth support services

### Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

### Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

## Department for Education (DfE)

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls, which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

## Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the main office at [schoolcontact@cityofrochesterschool.org](mailto:schoolcontact@cityofrochesterschool.org) for the attention of the Privacy and Compliance Officers (PCOs), Kieran Yates and Michelle Homer

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

### **Withdrawal of consent and the right to lodge a complaint**

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the main office at [schoolcontact@cityofrochesterschool.org](mailto:schoolcontact@cityofrochesterschool.org) for the attention of the Privacy and Compliance Officers (PCOs), Kieran Yates and Michelle Homer

### **Last updated**

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated in September 2023

### **Contact**

If you would like to discuss anything in this privacy notice, please contact: the main office at [schoolcontact@cityofrochesterschool.org](mailto:schoolcontact@cityofrochesterschool.org) for the attention of the Privacy and Compliance Officers (PCOs), Kieran Yates and Michelle Homer.

### **How Government uses your data**

The pupil data that we lawfully share with the Department for Education (DfE) through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

### **Data collection requirements**

To find out more about the data collection requirements placed on us by the Department for Education (DfE) (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

### **The National Pupil Database (NPD)**

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education (DfE) and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department for Education (DfE).

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

## Sharing by the Department for Education (DfE)

The law allows the Department for Education (DfE) to share pupils' personal data with certain third parties, including:

- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department for Education's (DfE) NPD data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department for Education (DfE) has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfе-external-data-shares>

How to find out what personal information the Department for Education (DfE) holds about you

Under the terms of the [Data Protection Act 2018](#), you are entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

To contact the Department for Education (DfE): <https://www.gov.uk/contact-dfe>

## Appendix 3:

*City of Rochester School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.*

### **The categories of school information that we process**

These include:

- personal information (such as name, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- driving licence and driving convictions information

This list is not exhaustive.

### **Why we collect and use workforce information**

We use workforce data to:

- a) enable the development of a comprehensive picture of the workforce and how it is deployed
- b) inform the development of recruitment and retention policies
- c) enable individuals to be paid

### **Collecting workforce information**

We collect personal information via employee questionnaires at the time of employment and during the year such as medical questionnaires, DBS checks, social media entries, safeguarding information

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with UK GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

### **Storing workforce information**

We hold data securely for the set amount of time shown in our data retention schedule.

### **Who we share workforce information with**

We routinely share this information with:

- our local authority (where applicable)
- the Department for Education (DfE)
- payroll providers
- EAP and OH providers

### **Why we share school workforce information**

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

### **Department for Education (DfE)**

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections

All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.



## Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the main office at [schoolcontact@cityofrochesterschool.org](mailto:schoolcontact@cityofrochesterschool.org) for the attention of the Privacy and Compliance Officers (PCOs), Kieran Yates and Michelle Homer

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

## Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the main office at [schoolcontact@cityofrochesterschool.org](mailto:schoolcontact@cityofrochesterschool.org) for the attention of the Privacy and Compliance Officers (PCOs), Kieran Yates and Michelle Homer

## Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated September 2023.

## Contact

If you would like to discuss anything in this privacy notice, please contact the main office at [schoolcontact@cityofrochesterschool.org](mailto:schoolcontact@cityofrochesterschool.org) for the attention of the Privacy and Compliance Officers (PCOs), Kieran Yates and Michelle Homer

## How Government uses your data

The workforce data that we lawfully share with the Department for Education (DfE) through data collections:

- informs the Department for Education (DfE) policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

## Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

## Sharing by the Department for Education (DfE)

The Department for Education (DfE) may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department for Education (DfE) has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the Department for Education (DfE) releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

## How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

To contact the Department for Education (DfE): <https://www.gov.uk/contact-dfe>