



DATA PROTECTION POLICY

May 2026

The policy was adopted by the governing body of New River College on 19th May 2026

Contents

1. Aims	3
2. Legislation & Guidance	3
3. Definitions	3
4. The Data Controller	4
5. Roles & Responsibilities	5
6. Data Protection Principles	6
7. Collecting Personal Data	6
8. Sharing Personal Data	7
9. Subject Access Requests and other Rights of Individuals	8
10. Parental requests to see Educational Record	10
11. Biometric Recognition Systems	10
12. CCTV	11
13. Photographs & Videos	11
14. Data Protection by Design & Default	12
15. Use of Generative AI Tools	12
16. Data Security & Storage of Records	13
17. Disposal of Records	14
18. Personal Data Breaches	14
19. Training	14
20. Privacy Notices	15
21. Monitoring Arrangements	15
22. Links with Other Policies	15
Appendix 1 – Personal Data Breach Procedure	16
Appendix 2 - Privacy notice for parents/ carers – use of your child’s personal data	19
Appendix 3 - Privacy notice for pupils	24
Appendix 4 - Privacy Notice for Staff	29
Appendix 5 – New River College Data Subject Access Request Flowchart	36

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 (UK GDPR) and the Data Protection Act 2018 (DPA 2018)

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation & Guidance

This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

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
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individuals': • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	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

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO under three separate references under the names: New River College, New River College Primary and New River College Medical and will renew these registrations annually or as otherwise legally required.

5. Roles & 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.

Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO's contact details are below:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (Option 1, then 1)

Executive Headteacher

The executive headteacher acts as the representative of the data controller on a day-to-day basis.

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 DPO 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

- 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 UK 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

a. 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 authority, 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 (DPA 2018).

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

a) 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. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing Personal Data

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
- 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.

The school may share pupil data with NHS or local authority immunisation teams under the lawful basis of public task and legal obligation. Only the minimum necessary data will be shared, and appropriate safeguards will be in place.

The school may share pupil data with NHS or local authority immunisation teams under the lawful basis of public task and legal obligation. Only the minimum necessary data will be shared, and appropriate safeguards will be in place.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

9. Subject Access Requests and other Rights of Individuals

a. 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 must be submitted in writing, either by letter or email to the DPO. 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 DPO.

b. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12):

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above):

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

c. Responding to subject access requests

When responding to requests, we:

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

See appendix 5 with a flowchart for NRC Subject Access Request.

We will not disclose information if:

- The request is manifestly unfounded or manifestly excessive (UK GDPR Article 12(5), as retained in UK law and amended, Applied via DPA 2018, section 3 and continued by DUA Act 2025), including:
 - Repeated requests where data has not changed
 - The request is linked to a demand for compensation, settlement, or another benefit
 - The request is submitted to harass, disrupt operations, or exert improper leverage
 - Compliance would impose an excessive burden / disproportionate effort (including external staffing), rendering the request manifestly excessive
- Disclosure would prejudice an investigation, regulatory function, or enforcement activity (DPA 2018, Schedule 2, Paragraph 2 — crime and taxation & Paragraph 7 — regulatory functions)
- The data is subject to legal professional privilege (DPA 2018, Schedule 2, paragraph 19)
- Disclosure would prejudice management forecasting, negotiations, strategic planning, or the conduct of the business (DPA 2018, Schedule 2, paragraph 22)
- A child with sufficient understanding objects to a parent-submitted request (DPA 2018, section 9 – children’s consent and capacity & DPA 2018, Schedule 3, paragraph 19 – child protection exemptions)
- Disclosure would be likely to cause serious harm to a child, young person or another individual (DPA 2018, Schedule 3, paragraph 19)
- Disclosure would infringe the rights and freedoms of others (DPA 2018, Schedule 3, paragraph 19)
- Exam scripts are exempt from access rights. Exam marks may be withheld only until results are announced (DPA 2018, Schedule 2, paragraph 25)
- 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.

d. 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 UK
- 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)
- The school will ensure that third-party data is redacted appropriately before responding to SARs
- Staff will be trained to recognize and escalate SARs promptly
- The school will maintain a log of SARs and responses to demonstrate compliance

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

10. Parental requests to see Educational Record

Parents have a right to access their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. The school may charge for hard copies. Biometric Recognition Systems

The school does not use biometric recognition systems, nor does it intend to use it in the immediate future.

If and where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also

obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

The School may use CCTV in various locations around the school site as an aid to safeguarding pupils and staff. If we use CCTV we will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Data Protection Officer (DPO).

12. Photographs & Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Pupils aged under 18 years of age

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, 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, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

13. Data Protection by Design & 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 DPO, 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 to rights and freedoms of individuals, and when introducing new technologies (the DPO 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 DPO 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

14. Use of Generative AI Tools

This section applies to the use of generative AI tools such as Microsoft Copilot, ChatGPT, or similar technologies that generate content based on user input. These examples are illustrative and not exhaustive.

In line with guidance from the Department for Education (DfE), schools may use generative AI tools to support teaching and administrative tasks, such as lesson planning, resource creation, marking, and feedback. However, AI must not replace teachers or be used to make decisions that significantly affect pupils without appropriate human oversight. Schools are responsible for ensuring that any use of AI complies with data protection, safeguarding, and intellectual property laws. The use of AI by pupils is at the school's discretion and must align with the school's acceptable use, academic integrity, and safeguarding policies.

Reference: Department for Education, "Generative Artificial Intelligence (AI) in Education", updated June 2025.

Where generative AI tools are used in school operations or teaching, the school will:

- Conduct a Data Protection Impact Assessment (DPIA) before use.
See Section 14: Data Protection by Design & Default for more on DPIAs.
- Avoid inputting identifiable personal data into AI tools, especially public-facing models.
- Ensure transparency with staff, pupils, and parents about how AI is used, including disclosing AI-generated content where appropriate.
- Ensure ethical use of AI: AI must not replace human judgment in decisions with legal or significant effects.
- Require meaningful human involvement in any decision-making process involving AI.

This aligns with Article 22 of the UK GDPR, which prohibits decisions based solely on automated processing that significantly affect individuals, unless specific safeguards are in place.

- Promote fairness: AI systems must be designed and deployed to avoid discriminatory or inequitable impacts.
- Ensure privacy: AI tools must not collect, store, or access personal data without consent or another lawful basis.
- Implement robust security measures to protect AI systems and data from unauthorised access or breaches.
- Update privacy notices to reflect the use of AI tools where personal data is processed.
- Maintain governance oversight through appropriate review and approval processes for AI use cases.
- Provide training to staff on the ethical and responsible use of AI, including data protection implications.
- Document the use of AI in outputs where applicable, e.g., *“This document was generated in part using Microsoft Copilot 365.”*
- Outputs generated by AI tools may contain inaccuracies, outdated information, or biased content. Staff must critically review all AI-generated material before use and remain responsible for its accuracy and appropriateness. The use of generative AI tools must comply with all applicable data protection laws, including the UK GDPR and the Data Protection Act 2018. Staff remain fully accountable for any content created or decisions made using AI tools. The use of AI does not transfer responsibility away from the individual or the school. Where AI tools are being piloted or evaluated, their use is subject to ongoing review and must follow any guidance issued by the school or governing body.

15. Data Security & 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
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards (except for the purposes of safeguarding and Pupil Passports where information can be displayed on staff room notice boards), or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety policy on acceptable use)
- 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)

16. Disposal of Records

NRC has a Records Management Policy 2026 which outlines the records the school maintains and the time of retention. The school maintains a data retention schedule in line with the Information and Records Management Society (IRMS) toolkit 2024. This schedule outlines how long different types of personal data are retained and ensures data is not kept longer than necessary.

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.

17. Personal Data Breaches

The school will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. For more detailed operational guidance, staff should refer to the school's full Data Breach Procedure document.

When appropriate, we will report the data breach to the ICO within 72 hours. Such 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 non-encrypted personal data about pupils

18. Training

All staff and governors 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.

19. Privacy Notices

The school will provide clear and accessible privacy notices to individuals at the point of data collection, explaining how their data will be used, stored, and shared. These notices will be reviewed regularly and updated as necessary (see Appendix 2, 3 and 4)

20. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary. Otherwise, this policy will be reviewed **every 2 years** and shared with the full governing board.

21. Links with Other Policies

This data protection policy is linked to other policies including:

- Freedom of information policy (Including publication scheme)
- Records Management Policy

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 (Option 1, then 1)

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO 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 DPO will alert the executive headteacher and the chair of governors
- The DPO 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 DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO 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 DPO 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 DPO must notify the ICO.

The DPO 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 by the DPO on the School's central systems.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO 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 DPO
 - 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

- If all the above details are not yet known, the DPO 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 DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO 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 DPO 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 DPO
 - 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 DPO 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 DPO 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 by the DPO on the Trust's central systems.

- The DPO and executive 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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
 - The DPO 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.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors

- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 - Privacy notice for parents/ carers – use of your child’s personal data

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing ‘privacy notices’ (sometimes called ‘fair processing notices’) to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**. We, New River College are the ‘data controller’ for the purposes of data protection law. Our data protection officer is Judicium Consulting Limited (see ‘Contact us’ below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. NRC follows the guidelines set out in the Information and Records Management Society's (IRMS) toolkit for schools. Please refer to the NRC Records Management Policy 2026.

Data sharing

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

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority; to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education; to meet statutory requirements to share certain information with it, such as the school census
- The pupil's family and representatives; to provide necessary information regarding their child and NRC
- Educators and examining bodies; for pupils to undertake public examinations and help them gain qualifications
- Our regulator; Ofsted; to meet NRC's statutory requirement to be assessed

- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations; to ensure NRC meets financial standards & regulations
- Central and local government; to enable NRC to effectively carry out the business of the School
- Our auditors; to ensure we meet audit regulations and statutory duties
- Survey and research organisations; Where non-personal data may contribute to improvements in education and to enable NRC to effectively carry out the business of the School
- Health authorities; To ensure the safeguarding and health needs of pupils
- Security organisations; To ensure the safeguarding and security of pupils, staff, volunteers and the public
- Health and social welfare organisations; To help with safeguarding and health needs of pupils and where we are legally obliged to share personal information following statutory legislation
- Professional advisers and consultants; to develop and facilitate effective teaching and learning and to enable NRC to effectively carry out the business of the School
- Charities and voluntary organisations; Where NRC have contracted them to provide necessary services.
- Police forces, courts, tribunals; when we are required to by Law
- Professional bodies; To enable NRC to effectively carry out the business of the School

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#) (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

Youth support services

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to Islington Council Youth Support Service, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to

request that we only pass the individual's name, address and date of birth to Islington Council Youth Support Service.

Transferring data internationally

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.

Parents and pupils' rights regarding personal data

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

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer (see below).

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 (Option 1, then 1)

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended for parents and to reflect the way we use data in this school.

Appendix 3 - Privacy notice for pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

We, New River College, are the 'data controller' for the purposes of data protection law.

Our data protection officer is named below. (see 'Contact us' below).

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law. NRC follows the guidelines set out in the Information and Records Management Society's (IRMS) toolkit for schools. Please refer to the NRC Records Management Policy 2026.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority; to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education; to meet statutory requirements to share certain information with it, such as the school census
- Your family and representatives; to provide them with necessary information about you and NRC
- Educators and examining bodies; to help enable you to do examinations and gain qualifications
- Our regulator, Ofsted; for them to check how NRC is doing
- Suppliers and service providers; so that they can provide the services we have contracted them for
- Financial organisations; to ensure NRC meets financial standards & regulations
- Central and local government; to enable NRC to carry out the business of the school
- Our auditors; To ensure we meet audit regulations and statutory duties
- Survey and research organisations; we may share non personal data to help make improvements in the school and in education in general
- Health authorities; to help meet your health & safeguarding needs

- Security organisations; where necessary to help with your safeguarding and security
- Health and social welfare organisations; to help with your safeguarding and health needs
- Professional advisers and consultants; to enable NRC to improve & effectively carry out the business of the School
- Charities and voluntary organisations; Where NRC have contracted them to provide necessary services.
- Police forces, courts, tribunals; when we are required to by Law
- Professional bodies; to enable NRC to effectively carry out the business of the School

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#), which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) if you have any questions about the database.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to Islington Council Youth Support Service, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to Islington Council Youth Support Service.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **‘subject access request’**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request, please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don’t want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don’t want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we’ve done something wrong.

You can make a complaint at any time by contacting our data protection officer (see below).

You can also complain to the Information Commissioner’s Office in one of the following ways:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 (Option 1, then 1)

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended to reflect the way we use data in this school.

Appendix 4 - Privacy Notice for Staff

Privacy Notice for Staff

This Privacy Notice applies to New River College. New River College is the data controller for the personal information collected. Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them.

This Privacy Notice explains how New River College collects, processes, holds and shares personal data about individuals we employ or otherwise engage to work in our school/organisation, in-line with our statutory responsibilities.

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by its employees and service providers in the performance of their duties.

1. Information that we collect, process and use

- personal information (such as name, employee or teacher number, national insurance number, bank account, address, contact details, date of birth, gender, next of kin and emergency contacts, nationality and entitlement to work in the UK, criminal record check);
- special categories of data for equal opportunities monitoring including characteristics information such as ethnic group and disability;
- contract information (such as the terms and conditions of employment; start dates, hours and days worked, post, tax, roles and salary / remuneration, including entitlement to benefits such as pensions);
- work absence information and annual leave (such as number of absences, including sickness absence, special leave and sabbaticals and the reasons for the leave);
- leave records (including maternity, paternity, adoption parental and shared parental leave);
- details of your qualifications (and, where relevant, subjects taught), skills, experience and employment history, including start and end dates, with previous employers;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including performance improvement plans and related correspondence;
- information about medical or health conditions, including disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership;
- copy of driving licence and passport;
- photographs (for example, ID cards, staff photo for the website and school notice board, recruitment packs etc);
- CCTV footage, for example: for safeguarding and disciplinary use.
- data about your use of the schools' information and communication system.

We collect this information in a variety of ways. For example, data is collected through application forms; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments (for example, team development/appraisals).

In some cases, we collect personal data about you from third parties. For example, references supplied by former employers and/or information from criminal records checks (known as DBS checks) permitted by law.

2. **Why we collect and use this information**

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed;
- improve the management of workforce data across the education sector;
- to enable us to meet our contractual and legal obligations,
- processing of teachers' pension and run recruitment and promotion processes and provide references on request for current and former employees;
- maintain accurate and up-to-date employment records;
- facilitate safe recruitment, as part of our safeguarding obligations towards pupils;
- support effective performance management in line with the schools' statutory duty;
- inform our recruitment and retention policies;
- allow better financial modeling and planning;
- enable equalities and equal opportunities monitoring;
- support the work of the School Teachers' Review Body (Regulatory Body).

3. **The lawful basis on which we process this information**

Personal information is collected from you in order to meet and discharge our contractual obligations and statutory duties as your employer.

If you fail to provide the personal information requested, amongst other things we may not be able to provide you with employment or a service for which you may be entitled/requested.

The legal basis for the use of your personal data will be one or more of the following:

- to satisfy our legal obligations and statutory duties as your employer.
- to carry out a task in the public interest or in the exercise of official authority in our capacity as a school.
- to meet our contractual obligations in relation to your statement of employment contract with us.

4. **Collecting workforce information**

We collect personal information via: application forms, pre-employment documents, HMRC starter check list, references and staff contract form.

Workforce data is essential for the school's / local authority's operational use.

Whilst the majority of information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with 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 and we will tell you what you need to do if you do not want to share this information with us.

5. **Storing this information**

Data is stored in a range of different places, included in your school personnel file, on the single central record, SIMS, the IT system of the schools HR and Payroll provider, and in other IT systems (including the schools email system). The information is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete information in it in accordance with the School's Records Management Policy / retention policy.

6. Who we share your information with

We do not share information about you without your consent unless the law and our policies allow us to do so.

We may share your personal information with the following organisations who are also Data Controllers.

Our Local Authority London Borough of Islington	We are required to share information about our workforce members with our local authority (LA) pursuant to s 5 the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments
The Department for Education (DfE)	We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment. The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005 To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools. For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data All data is transferred securely and held by 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.
London Borough of Islington	We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

The Department for Education (DfE)	We are required to pass information about our pupils to the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005 To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools. For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
------------------------------------	--

We may also share your information, with the following:

- Your family or representatives
- Police forces, courts, tribunals

Function	Contact details
Educators and examining bodies	These include AQA, Pearson Edexcel, WJEC, JCQ for pupils to undertake public exams
Regulatory Bodies	Ofsted
Suppliers and services providers – to enable them to provide the service we have contracted them for, such as payroll, ICT	Islington Schools HR, Islington Schools Payroll, London Borough of Islington, RM, Schools ICT, Engie
Central and local government	DfE, London Borough of Islington
Our auditors	This is to ensure we meet financial statutory regulations
Survey and research organisations	Varied
Trade unions and associations	NEU, Unison, GMB and any other union staff are members of
Health Authorities	Islington PCT, Whittington NHS Trust

Security organisations	All NRC sites use CCTV and this is serviced and maintained by several contractors
Health and social welfare organisations	CAMHS, School Nurse Service, Islington CSC
Professional Advisors and consultants	NRC contract the services of a number of advisors and consultants including School Improvement Partner (SIP), Islington Schools Improvement
Charities and voluntary organisations	As a School we gain various sources of funding
Professional bodies	The School is a member of various professional bodies including PiXL
Employment and recruitment agencies	The School use various providers to recruit staff

7. 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:

Mark Gilleran, Business Manager,
New River College
Lough Road
London
N7 8RH
Email: mark.gilleran@nrc.islington.sch.uk
Telephone: 020 7504 0543 option 2

Or our Data Protection Officer: see contact details at item number 9 below.

In some circumstances you may also have the right to ask:

- us to restrict the processing of your personal data until any errors are corrected,
- to object to our processing or transferring of your personal data.
- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern or query about the way we are collecting or using your personal data, we ask that you raise your concern/query with us in the first instance on the contact details below. 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 DfE, please see the 'How Government uses your data' section of this notice.

8. 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 on 7th October 2024.

9. **Contact**

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- 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, you should make a 'subject access request'. Further information on how to do this can be found within the Department's 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: <https://www.gov.uk/contact-dfe>

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (Option 1, then 1)

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

10. **Your other rights over your data**

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- 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, you should make a 'subject access request'. Further information on how to do this can be found within the Department's 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: <https://www.gov.uk/contact-dfe>

11. **How Government uses your data**

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental 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 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

The Department 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 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 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 DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- 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, you should make a 'subject access request'. Further information on how to do this can be found within the Department's 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: <https://www.gov.uk/contact-dfe>

Appendix 5 – New River College Data Subject Access Request Flowchart

