DOWNSVIEW PRIMARY SCHOOL

DATA PROTECTION AND RECORDS MANAGEMENT POLICY

Originator: Carol Christodoulou
Approved by: Governing Board 18th October 2024
Revision Date: October 2026

Downsview Primary School
Biggin Way
Upper Norwood
London
SE19 3XE

Telephone: 020 8764 4611
Email: sec1@downsview.croydon.sch.uk
Webpage: www.downsview.croydon.sch.uk

Contents:

1. Statement of Intent

Downsview Primary and Nursery School is required to keep and process certain information about its staff, pupils, parents, governors, visitors and other individuals who come into contact with the school, in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

The UK GDPR ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The school collects and uses personal information about staff, pupils, parents, governors, visitors and other individuals who come into contact with the school. Personal data is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

This policy sets out how the school handles personal data and applies to all personal data, regardless of whether it is in paper or electronic format. This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the core principles of the UK GDPR. Organisational methods for keeping data secure are imperative, and the school believes that it is good practice to keep clear practical policies, backed up by written procedures.

All staff involved with the collection, processing and disclosure of personal data 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.

The school is registered as a Data Controller with the Information Commissioner's Office (ICO) detailing the information held and its use and will continue to pay its registration fee annually or as otherwise legally required.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the local authority, other schools and educational bodies and potentially children's services.

2. Legal Framework and Guidance

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act (DPA) 2018

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.

This policy will be implemented in conjunction with the following other school policies:

- Data Retention Policy
- CCTV Policy
- AI Policy
- Breach Policy and Procedures
- Online Safety, Social Media, Devices and Acceptable Use Policy
- IT Security Policy
- Freedom of Information Policy
- Protection of Biometric Information of Children Policy

3. Definitions and Applicable Data

This policy makes reference to the following definitions:

TERM	DEFINITION
Personal data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. For the purpose of this policy, Personal Data refers to information that relates to an identifiable, living individual, including an individual's name (including initials), identification number, location data and online identifiers, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.
Special categories of personal data and Data Relating to Criminal Convictions and Offences	Previously termed Sensitive Personal Data, Special Category Data refers to data concerning an individual data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data. Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
Processing	Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.
Automated Processing	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

TERM	DEFINITION
Data subject	An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.
Data controller	The organisation storing and controlling such information (i.e., the School) is referred to as the Data Controller.
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.
Pseudonymised	The process by which personal data is processed in such a way that that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.
Data Protection Impact Assessment (DPIA)	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

4. Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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.

5. Accountability

The School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. The school will also provide comprehensive, clear and transparent privacy policies.

The School is required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the School
- The name and contact details of the Data Protection Officer
- Descriptions of the types of personal data used
- Description of the data subjects
- Details of the School's processing activities and purposes
- Details of any third party recipients of the personal data
- Where personal data is stored
- Retention periods
- Security measures in place

6. Roles and Responsibilities

Governing Board
The Governing Board has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

Data Protection Officer (DPO)
A DPO has been appointed in order to monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments and conducting data protection audits. The DPO has professional experience and knowledge of data protection law, particularly that in relation to schools. They will provide an annual report of their activities to the highest level of management at the school and, where relevant, make recommendations on school data protection issues. The DPO will operate independently and will not be dismissed or penalised for performing their task. Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

The school's DPO is Judicium Consulting Limited and is contactable via the following methods:

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 option 1 again

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

All Staff
All staff are expected to read, understand and comply with this Policy. 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 or contact details.

7. Lawfulness, Fairness and Transparency

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- An individual (or their parent/carer in the case of a pupil) has freely given clear consent.
- Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person, e.g. to protect someone's life.
- For the purposes of legitimate interests pursued by the Data Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways that have unjustified adverse effects on them.

8. Consent and Sharing Personal Data

Where required, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given.

The school will ensure that consent mechanisms meet the standards of the UK GDPR. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained. Consent can be withdrawn by the individual at any time.

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 UK data protection law
- Establish a contract with the supplier or contractor 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

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

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 internationally, we will do so in accordance with UK data protection law.

9. The Right to be Informed

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The School's privacy notices are tailored to suit the data subject and set out information about how the School use their data.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the school's Privacy Notices:

- The identity and contact details of the Data Controller and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- Details of where to find the retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to withdraw consent at any time and/or lodge a complaint with a relevant supervisory authority.
- The existence of any automated decision making, including profiling, how decisions are made, the significance of the process and the consequences, where applicable.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be:

- Published on the school website.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. Subject Access Requests and Other Rights of Individuals

Individuals have a right to make a Subject Access Request (SAR) to gain access to personal information that the school currently holds on file 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
- Confirm how long the data will be stored for
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

The school's procedures for processing Subject Access Requests are detailed in **Appendix 1**.

In addition to data protection law, pupils and parents also have separate rights to access to Educational Records under Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 (EPIR). In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations. If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

11. The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification, where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority.

12. The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The Right to Restrict Processing

Individuals have the right to block or suppress the school's processing of personal data in certain circumstances. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data

- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

14. The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes. The school will ensure that personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school is not required to adopt or maintain processing systems that are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

15. The Right to Object

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received. The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

16. Automated Decision Making and Profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The school does not use automated decision making or profiling in its activities.

17. Privacy by Design and Data Protection Impact Assessments

The school will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures, which demonstrate how the school has considered and integrated data protection into 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)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- The school will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The school regularly test its data systems and processes in order to assess compliance. These are done through data audits by the DPO, which take place annually in order to review use of personal data. Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

- Completing data protection impact assessments (DPIAs) 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).

The School carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

18. Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The school will make all reasonable endeavours to ensure that there are no personal data breaches.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the DPO will notify the Information Commissioner's Office within 72 hours of the school becoming aware of it. In the event that a breach is sufficiently serious, those involved will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or those involved need to be notified.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator, where we are legally required to do so. Please refer to the school's Data Breach policy for further details. In the event that safeguarding information is compromised, the school's Data Team will inform the school's Designated Safeguarding Lead who will decide whether the school should inform the DPO and its local safeguarding partners, as appropriate.

19. Data Security

The school will protect 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:

- Confidential paper records will be locked away, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- School phones (landline and school mobile phones allocated to staff) must be used for all school purposes including emergency calls. Parent contact numbers should not be saved on staff personal mobiles. When children undertake a school trip or journey, the school's mobile phone should be used. If necessary, staff participating on a school trip may use their own phone, but for the limited purpose to contact the other adults in the group, the school office, or the venues being visited or an emergency number, if necessary. Parent contact numbers are stored on the school's After School Club mobile to allow staff to contact parents when waiting for parents to collect at the end of the After School Club. All school mobiles are PIN protected and staff who are allocated a mobile phone must not share the PIN.
- Circular emails to parents are sent blind carbon copy (bcc) from the school's email messaging service or the school's main email address, so that email addresses are not disclosed to other recipients. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- 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.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Recipient(s) of the data have been outlined in the relevant school Privacy Notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/theft is identified, extra measures to secure data storage will be put in place.

The school takes its duties under the UK GDPR seriously and all members of staff are required to familiarise themselves with the content of this Policy and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence, which may result in disciplinary action under the School's Disciplinary Policy and Procedures.

The school has continuity and recovery measures in place to ensure the security of protected data.

20. Publication of Information

The school will not publish any personal information, including photos or video recordings, on its website without a parent or employee's consent.

21. Photography and CCTV

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles..

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

The school will always indicate its intentions for taking photographs and recorded images and will obtain parental consent before publishing/displaying them on school noticeboards, in communication materials, for promotional and marketing purposes and on the school website or on social media. The school will clearly explain how photographs and/or video recordings will be used. Precautions, as outlined in the Acceptable Use Policy are taken when publishing photographs of pupils, in print or video.

Consent can be refused or withdrawn at any time.

Images captured by individuals for recreational/personal purposes, and videos made by parents/carers for family use, are exempt from the UK GDPR. However, we request that any such photographs or video recordings of any school event, are kept for family use only and are not shared in the public domain, including social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

The school uses CCTV in various locations around the school site to ensure it remains safe. The use of CCTV is detailed in our CCTV Policy.

22. Artificial Intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The school recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, and in line with the school's AI Policy, neither staff or pupils are permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the school will treat this as a data breach, and will follow the personal data breach procedure outlined in the school's Data Security Breach Prevention Policy and Data Breach Procedure.

23. Data Retention Policy

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. Details of the school's retention periods can be found in the school's Data Retention Policy.

The Data Retention Policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained for a set period to provide evidence of its transactions or activities.

Records will not be kept for longer than is necessary. The school follows the Information and Records Management Society's Retention Guidelines for Schools. Unrequired data will be deleted, in line with the school's Data Retention Policy, as soon as practicable. Staff must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Policy.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

24. 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. Paper documents will be shredded and electronic files deleted. 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.

25. DBS Data

All data provided by the Disclosure and Barring Service (DBS) will be handled in line with data protection legislation; this includes any electronic communication in relation to DBS checks.

26. Policy Review

This policy is reviewed every two years. The next scheduled review date for this policy is July 2025.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be made to the Information Commissioner (ICO).

APPENDIX 1 Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the school holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data Subject Access Request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the school are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the school at potentially significant risk and so the school takes compliance with this policy very seriously.

A data subject has the right to be informed by the school of the following:

a) Confirmation that their data is being processed.
b) Access to their personal data.
c) A description of the information that is being processed.
d) The purpose for which the information is being processed.
e) The recipients/class of recipients to whom that information is or may be disclosed.
f) Details of the school's sources of information obtained.
g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct, and
h) Other supplementary information.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, the school has only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay.
All staff are made aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the school may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the school.

If a staff member receives a SAR, they must notify the School Business Manager. A request for information does not need to mention that it is a SAR, provided that it is clear that it is an individual asking for their own personal data (or in the case of a parent/carer the personal data of their child). There is no specified wording and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media, where relevant.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent/carer making a request in relation to information relating to their child):

- For confirmation as to whether the school process personal data about him/her and, if so
- For access to that personal data
- And/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the school to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request, which may delay the start of the time period for dealing with the request.

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the School Business Manager, who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the school must respond to a request, and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. If ever in doubt, please refer the request to DPO.

Acknowledging the Request

When receiving a SAR the school shall acknowledge the request, as soon as possible, and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the school may ask for:

- Proof of ID (if needed).
- Further clarification about the requested information if it is not clear what information is required.
- If it is not clear where the information shall be sent, the school must clarify what address/email address to use when sending the requested information and/or
- Consent (if requesting third party data).

The school should work with their DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the school will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the school has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the school may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know, as soon as possible, where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

Requests Made by Third Parties or on Behalf of Children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The school may also require proof of identity in certain circumstances.

If the school is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else, such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the school should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- The child's level of maturity and their ability to make decisions like this.
- The nature of the personal data.
  Any court orders relating to parental access or responsibility that may apply.
- Any duty of confidence owed to the child or young person.
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information and
- Any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the school is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the school will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee for Responding to a SAR

The school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive, a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable, the school will inform the requester why this is considered to be the case and that the school will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances, a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the school is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the school may be closed and no one will be on site to comply with the request. As a result, it is unlikely that requests will be able to be dealt with during this time. We may not be able to acknowledge requests during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the school re-opens. The school will endeavour to comply with requests as soon as possible and will keep in communication with the requestor, as far as possible. If a request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about them and the following information:

- The purpose for which we process the data.
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations.
- Where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The fact that the individual has the right:

- to request that the school rectifies, erases or restricts the processing of their personal data, or
- to object to its processing,
- to lodge a complaint with the ICO, and
- where the personal data has not been collected from the individual, any information available regarding the source of the data.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the school are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the school have one month in which to respond, the school is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied, if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the school is allowed to carry out regular housekeeping activities, even if this means deleting or amending personal data after the receipt of a SAR. The school is not allowed to amend or delete data to avoid supplying the data.

Locate Information

The personal data the school need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the school may need to search all or some of the following:

- Electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV.
- Manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data.
- Data systems held externally by our data processors.
- Safeguarding systems (such as CPOMS).
- MIS system (such as SIMS).
- Occupational health records.
- Pensions data

The school should search these systems using the individual's name, initials, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The school will consider whether it is possible to redact information, so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to), then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- The other individual has consented to the disclosure, or
- It is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- The type of information that they would disclose.
- Any duty of confidentiality they owe to the other individual.
- Any steps taken to seek consent from the other individual.
- Whether the other individual is capable of giving consent.
- Any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances, the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The school do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The school do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- Education, training or employment of the individual
- Appointment of the individual to any office
- Provision by the individual of any service

This exemption does not apply to confidential references that the school receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the school must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The school do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The school do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The school do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual, where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The school can refuse to comply with a request if the request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive*,* taking into account whether the request is repetitive in nature.
- To avoid obstructing an official or legal inquiry, investigation or procedure.
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.
- To protect public security.
- To protect national security.
- To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to DPO who will make the decision on our behalf.

In the event that we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive, the school can:

- request a reasonable fee to deal with the request; or
- refuse to deal with the request.

In either case, the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record Keeping

A record of all subject access requests shall be kept by the School Business Manager. The record shall include the date the SAR was received, the name of the requester, what data the school sent to the requester and the date of the response.

Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the **details of the data subject** below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records: If you are, or have been employed by the school and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc. Details:

Section 2

Please complete this section of the form **with your details if you are acting on behalf of someone else** (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity, as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to sec1@downsview.croydon.sch.uk