Purley Partnership Federation

Purley Nursery School
Achieving and growing together

Christ Church Primary School
Nurturing lifelong learners with God's guidance

General Data Protection Regulation & Freedom of Information Policy

Reviewed July 2026, to be reviewed July 2029

Introduction
The UK General Data Protection Regulation (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 Schools will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, governors, volunteers and any other third parties. This policy does not form part of any individual's terms and conditions of employment with the Schools and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Staff is defined by employees, governors, trustees and volunteers. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Federation's Disciplinary Policy and Procedure up to and including dismissal depending on the seriousness of the breach.

The Schools are registered with the Information Commissioner's Office (ICO) as required and registration numbers are:

Christ Church Primary School: Z4875401
Purley Nursery: Z7123248

Section 1 – Definitions

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. 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.
Special	Previously termed "Sensitive Personal Data", Special Category Data is

Category Data and Data Relating to Criminal Convictions and Offences	similar by definition and 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.
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.
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. Examples of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing (without meaningful human intervention).
Data Protection Impact Assessment (DPIA)	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.
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 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.

Section 2 – When can the School Process Personal Data?

The Federation is responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the Schools must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Schools only collect, process and share personal data fairly and lawfully and for specified purposes.

The Schools must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

The Schools may only process a data subject's personal data if one of the following lawful bases are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the Schools' legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.
- The processing is necessary for a recognised legitimate interest under the UK GDPR (as amended by the Data (Use and Access) Act 2025).

Special Category Data

The Schools may only process special category data if they are entitled to process personal data (using one of the lawful bases above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Schools in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;

- To protect the data subject's (or another person's) vital interests, where the data subject is unable to give consent;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The Schools identify and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the Federation relies on consent as a lawful basis for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The Schools will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any manner that is incompatible with the legitimate purposes specified.

The Schools will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Schools will only process personal data when our obligations and duties require us to. We will not collect excessive data and will ensure any personal data collected is adequate and relevant for the intended purposes.
When personal data is no longer needed for specified purposes, the Schools shall delete or anonymise the data as per the Data Retention policy

Principle 4: Personal data must be accurate and, where necessary, kept up to date
The Schools will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Schools.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Schools will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.
Please refer to the School's Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to ensure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (as outlined above);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Schools follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.
The Schools will only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data
The Schools will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the Schools are required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within written notifications, including details and the basis for sharing the data. Further information can be found in the privacy notice.

Transfer of Data Outside the UK
The UK GDPR restricts the transfer of personal data to countries or international organisations outside of the UK to ensure that individuals' data continues to receive an adequate level of protection.
The School will not transfer personal data outside of the UK unless:

- the destination country is covered by a UK adequacy regulation;
- appropriate safeguards are in place, such as a UK International Data Transfer Agreement (IDTA) or an approved set of standard contractual clauses, and enforceable data subject rights and effective legal remedies are available;
- a specific derogation applies under Article 49 UK GDPR (for example, the transfer is necessary for an important reason of public interest).

All staff must comply with the Schools' guidelines on transferring personal data outside of the UK. For clarity, a "transfer" may occur whenever personal data are sent, accessed, viewed, or otherwise made available from outside the UK.

The Schools monitors any international transfers with support from the Data Protection Officer (DPO) and maintain records of our transfer assessments alongside a Third-Party Data Sharing Register.

Section 3 – Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Schools handle their personal data are set out below:

A. To withdraw consent to processing at any time (where consent is relied upon as a condition of processing);
B. Receive certain information about the School's processing activities;
C. Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);
D. Prevent our use of their personal data for direct marketing purposes;
E. Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
F. Restrict processing in specific circumstances, such as where the accuracy of the data is contested or an objection is being considered
G. Challenge processing which has been justified on the basis of legitimate interests or in the public interest;
H. Request a copy of an agreement under which personal data is transferred outside of the UK;
I. To be informed where decision that has legal or similarly significant effects is made solely by automated means, and to request human intervention, express their point of view, or contest a decision;
J. Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
K. To raise a concern or make a complaint directly to the School if they believe their personal data has been processed unlawfully or unfairly, or if they are dissatisfied with the School's response to a data protection request. Individuals also have the right to make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales (https://ico.org.uk/global/contact-us/); and
L. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

Direct Marketing

The Schools are subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Schools will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

Employee Obligations
Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Schools in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction;
- Not remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

Section 4 - Accountability
The Schools will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The Schools have taken the following steps to ensure and document UK GDPR compliance:-

Data Protection Officer (DPO)
Please find below details of the School's 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 option 1 again)

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.
Should staff have any questions about the UK GDPR, the operation of this policy or, if you have any concerns that this policy is not being, or has not been, followed, please contact ECT or HoS in the first instance. Should the matter remain unresolved or require further escalation, please contact the school's DPO.

In particular, you can contact the DPO in the following circumstances:

1. If you are unsure of the lawful basis being relied on by the School to process personal data;
2. If you need to rely on consent as a lawful basis for processing (please see below the section on consent for further detail);
3. If you need to draft privacy notices or policies;
4. If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Retention Policy in the first instance];

5. If you are unsure about what security measures need to be put in place to protect personal data;
6. If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Breach Policy];
7. If you are unsure on what basis to transfer personal data outside the UK;
8. If you need any assistance dealing with any rights invoked by a data subject;
9. Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
10. If you plan to undertake any activities involving automated processing or automated decision making;
11. If you need help complying with applicable law when carrying out direct marketing activities;
12. If you need help with any contracts, data processing agreements or other areas in relation to sharing personal data with third parties.

Data Subject Complaints

Individuals have the right to make a complaint directly to us if they believe their data protection rights have been breached.

We will acknowledge receipt within 30 days and provide a substantive response without undue delay. If you are not satisfied with our response, you may escalate the matter to the Information Commissioners Office (ICO).

Further information about how the Trust handles data protection complaints can be found at Appendix 3 of this policy, along with a data protection complaints form at Appendix 4. Complaints can be made in writing to the EHT (head@christchurch.croydon.sch.uk) or HoS (head@purley.croydon.sch.uk)

Personal Data Breaches

The UK GDPR requires the Schools to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We will 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.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (SBM at Christ Church or HoS at Purley Nursery School) or the School DPO.

Transparency and Privacy Notices

The Schools will provide detailed, specific information to data subjects. This information will be provided through the Federation'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 Federation's privacy notices are tailored to suit the data subject and set out information about how the Schools use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

Privacy by Design

The Federation adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Schools take into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Schools conduct DPIAs for any new high-risk technologies or programmes being used by the School which could affect the processing of personal data. The Schools carry 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 (for example, 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.

Record Keeping

The Schools are required to keep full and accurate records of our data processing activities (Records of Processing Activities (ROPA)). 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; and
- Security measures in place.

Training
The Schools will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The school will carry out adequate training with all staff annually and at induction with new staff.

Audit
The School, through its Data Protection Officer, regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

Related Policies
This policy should be read in conjunction with the:

- Data Retention Policy
- Code of Conduct
- Safeguarding Policy
- School Teachers Pay and Conditions Document
- Equal Opportunities and Race Equality Policy
- SEND Policy
- Learning and Teaching Policy
- General Data Protection Regulation (2018)
- Parent, Staff and Pupil Privacy Notices for the Purley Partnership Federation
- AI policy

Monitoring
We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Schools.

Section 5 – Automated Processing and Automated Decision Making
Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision-making for significant decisions and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision-making are limited.

You will not be subject to automated decision-making for significant decisions unless we have a lawful basis for doing so, including a valid condition where required, and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision-making and their rights to request a human review, express their views, and contest the decision.

The School will carry out a data protection impact assessment before any new automated processing or automated decision-making activities are undertaken.

APPENDIX 1 Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process 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: -

1. Confirmation that their personal data is being processed;
2. Access to their personal data;
3. The following 'supplementary information':
    a. The purposes of processing;
    b. The categories of personal data concerned;
    c. The recipients or categories of recipients to whom the data have been or will be disclosed;
    d. Where possible, the period for which the data will be stored, or the criteria used to determine that period;
    e. The existence of the data subject's rights to rectification, erasure, restriction, objection and data portability;
    f. The right to lodge a complaint with the ICO;
    g. Where the data were not collected directly from the individual, any available information about the source;
    h. Any automated decision-making, including profiling, and information about the logic involved, as well as the significance and envisaged consequences of such processing; and,
    i. Where relevant, details of the safeguards applied to data transferred outside the UK.

Dealing with a SAR is time-critical and must be prioritised. Other than in exceptional cases, we will have 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. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be 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 Schools 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 schools
.
If you receive a SAR, please contact EHT, HoS or SBM. 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. 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 making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information (listed above).

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 holds 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 Schools 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 in turn 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 SBM who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the Schools 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 EHT/HoS.

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 Schools will take reasonable steps to verify the identity of the person making the request. In the case of current employees and current students, this will usually be straightforward. The Schools are 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 Schools have 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 required to confirm 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 may be paused 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 schools 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 Schools may also require proof of identity in certain circumstances.

If the Schools are 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 Schools 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 Schools 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 Schools are 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 Schools will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The Schools 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 Schools 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 Schools will inform the requester why this is considered to be the case and that the Schools may 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 Schools have 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. If the deadline to comply with the request falls on the weekend or public holiday, the deadline will be the next working day.

The circumstances where the Schools are 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 schools 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 Schools 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 schools 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 no one will be on site to comply with the request. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request 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 Schools will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your 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 him or her and the supplementary information listed above.

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. Where a request is made by electronic means, and unless the requestor asks otherwise, the Schools will normally provide the information in a commonly used electronic format (for example, PDF). The format of the response will reflect the method of

the request where reasonable and appropriate, unless the requestor specifies another preferred, reasonable and appropriate, format.

The information that the Schools 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 Schools have one month in which to respond the Schools are 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 Schools are 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.

How to 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, MyConcern);
- MIS system (such as SIMS, Bromcom, Arbor);
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

We will handle data subject rights requests and searches in a manner that is reasonable and proportionate to the nature of the request, the amount of data involved, and the effort required. We will not conduct searches that would impose a disproportionate burden on our operations where this would go beyond what is reasonable to locate personal data.

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 Schools 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 Schools 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; and
- 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, or received from, third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

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

Management forecasting: The Schools 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, to the extent that disclosure of the information would be likely to prejudice the conduct of the School's business or other activity.

Negotiations: The Schools 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 EHT/HoS 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 EHT and HoS. The record shall include the date the SAR was received, the name of the requester, what data the Schools sent to the requester and the date of the response.

Appendix 2 – 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 document):

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 document):

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: office l@christchurch.croydon.sch.uk

office@purley.croydon.sch.uk

Appendix 3 – Data Protection Complaints

Under Data Protection Law, individuals have the right to raise concerns or make complaints about the way their personal data has been handled. This includes concerns about how the School collects, stores, uses, shares, or secures personal data, as well as how the School has responded to a previous data protection related request (for example, a Subject Access Request).

The purpose of this right is to ensure that individuals can easily challenge potential non-compliance, seek clarification or correction, and help the School to continually improve its data protection practices.

This appendix provides guidance for staff on how to handle data protection complaints and for individuals on how to submit one.

Failure to address data protection complaints appropriately can expose the School to enforcement action by the ICO and reputational risk. The School therefore treats all complaints seriously and in accordance with this policy.

What is a Data Protection Complaint?

A data protection complaint is any expression of dissatisfaction from an individual (or their authorised representative) about how the School has processed their personal data or handles a data protection request.

Examples include complaints about:

- Inaccurate, incomplete, or outdated information being held;
- Personal data being used or shared without lawful basis;
- A delay or failure to respond to a Subject Access Request or other data rights request;
- Inappropriate disclosure or loss of personal data;
- Lack of transparency in how data is collected or used;
- Concerns about automated decision-making or profiling; or,
- Any other alleged breach of the UK GDPR or Data Protection Act 2018.

A complaint does not need to reference "data protection" or "UK GDPR" to be valid; any statement indicating concern about how personal data has been handled must be treated as such.

How to Make a Data Protection Complaint

Individuals can make a complaint verbally or in writing (including by email, letter, or online form). To help ensure a full and efficient investigation, complainants are encouraged to use the Data Protection Complaint Form provided below in Appendix 4, providing:

- Their name and contact details;

- A clear description of the concern;
- Any relevant dates, correspondence, or evidence; and,
- The outcome they seek.

Complaints should be directed to EHT at Christchurch Primary school or the HoS at Purley Nursery School.

Acknowledging and Investigating a Complaint:

The School will acknowledge the complaint within 30 days of receipt. The acknowledgment will confirm that the complaint has been received, outline the next steps, and provide contact details for any questions.

Where clarification or additional evidence is required to investigate the complaint properly, the response timeframe may be paused until sufficient information has been provided. All complaints will be handled confidentially and investigated promptly, fairly, and proportionately.

The School will aim to provide a substantive response as soon as reasonably practicable. The investigation may involve consultation with relevant departments, review of systems or records, and advice from the School DPO.

Outcome of a Complaint

Following investigation, the School will provide a written response setting out:

- The findings of the investigation;
- Any corrective or preventative action the School will take (if appropriate); and,
- The right to escalate the matter to the ICO if the complainant remains dissatisfied.

Complaints Received During School Closure Periods

The School will endeavour to acknowledge and investigate complaints as soon as reasonably practicable. However, during school closure periods, offices and systems may not be routinely monitored, which could delay acknowledgment and investigation. Where a complaint is received during such a period, the School will:

- Record the date of receipt;
- Acknowledgment the complaint as soon as possible; and,
- Provide an update to the complainant once the School reopens.

Complainants who require an urgent response are encouraged to submit their complaint during term time wherever possible.

Record Keeping

The School will maintain a record of all data protection complaints, including:

- The date the complaint was received;
- The complainant's name;
- The nature of the complaint;
- Any key investigative steps taken;
- The outcome and date of response; and,
- Any follow-up actions taken.

Records will be retained in accordance with the School's Records Retention Schedule.

Appendix 4 – Data Protection Complaints Form

The UK GDPR and the Data Protection Act 2018 give you the right to raise a concern or make a complaint about the way the School processes your personal data, handles your request, or otherwise complies with data protection law.

Please complete this form if you wish to raise a complaint and send it to EHT at Christchurch Primary School or the HoS at Purley Nursery School. The School will acknowledge your complaint within 30 calendar days of receipt and will aim to provide you with a full response as soon as reasonably practicable.

Proof of Identity

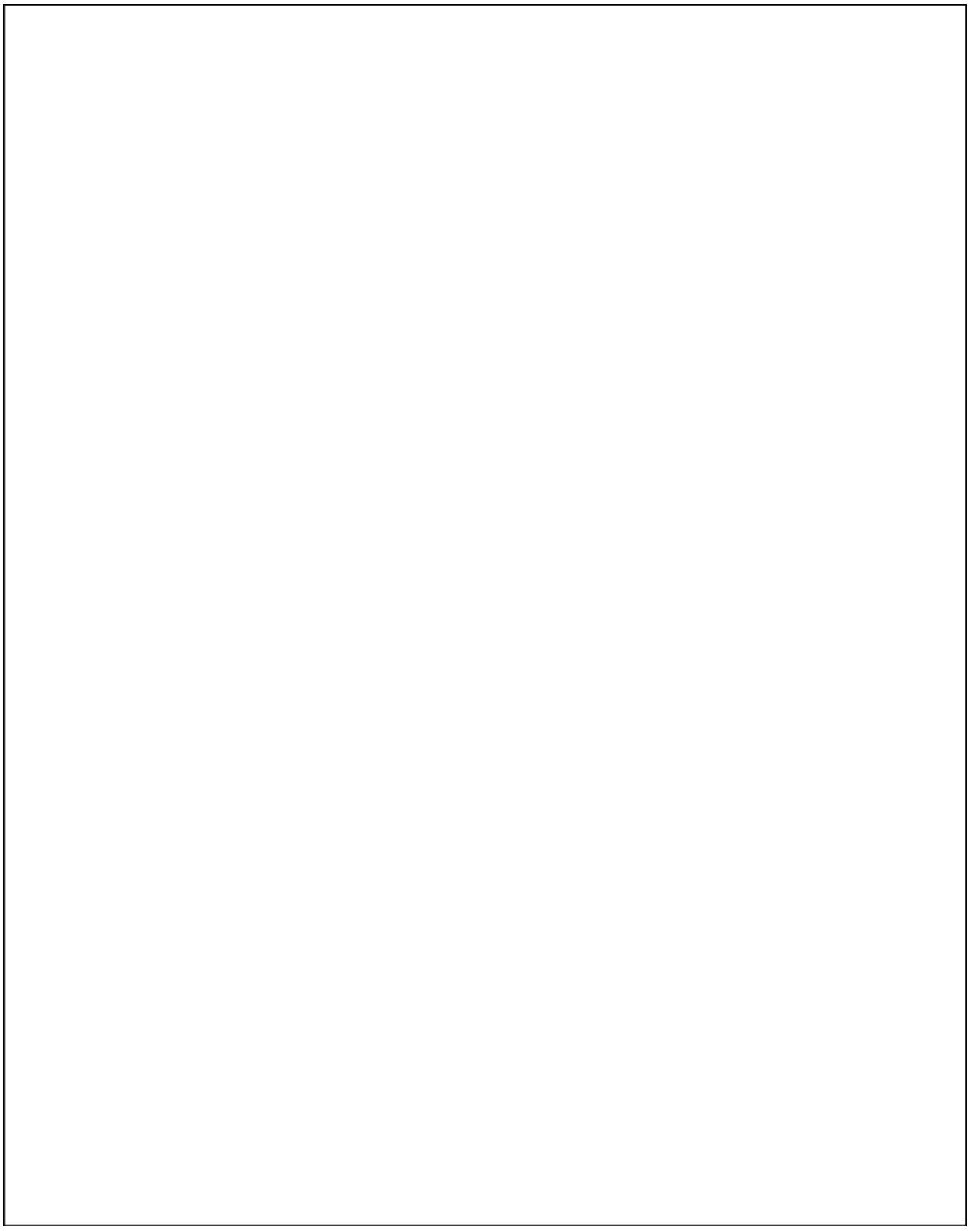
If your complaint relates to the processing of personal data and we need to verify your identity, we may ask for proof of identity before investigating. Acceptable documents include a copy of your passport, driving licence.

Section 1 – Complainant Details

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

Section 2 – Details of Complaint

Please describe your concern in as much detail as possible. Include dates, names, and copies



of any relevant correspondence or documents if available.

Have you previously raised this concern with the School?

☐ Yes ☐ No

If yes, please provide the date and to whom it was reported:

What outcome are you seeking?

Section 3 – Representative (if applicable)

If you are making this complaint on behalf of someone else, please complete the section below.

You must provide proof of your identity and evidence of your authority to act on behalf of the data subject.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	

Post Code	
Phone Number	
Email address	
Relationship to Data Subject	

Proof of Authorisation (enclose one):

☐ Letter of authority ☐ Power of Attorney ☐ Parental responsibility ☐ Other (details): _____

Section 4 – Acknowledgement and Declaration

☐ I confirm that the information provided in this form is accurate to the best of my knowledge.
☐ I understand that the School may need to contact me to clarify details and may need to verify my identity before investigating.

Signature: _____ Date: _____

Freedom of Information Policy

Introduction

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information. Full details on how requests can be made are set out in section 1 of this policy.

Public authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available and can be found at section 2 of this policy.

This policy does not form part of any individual's terms and conditions of employment with the School [LK1] and is not intended to have contractual effect. This policy should be used in conjunction with the School's Data Protection Policy.

Section 1 – Freedom of Information Requests

Requests under Freedom of Information should be made to the EHT/HoS. However, the request can be addressed to anyone in the School. All staff need to be aware of the process for dealing with requests. If staff receive a FOI request in their inbox, it should be instantly forwarded to EHT/HoS.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act.

Data protection enquiries (or Subject Access Requests/SARs) are requests where the enquirer asks to see what personal information the school holds about the enquirer. If the enquiry is a data protection request, the School's Data Protection Policy should be followed.

Environmental Information Regulations enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, health and any decisions and activities affecting any of these. These could, therefore, include enquiries about recycling, phone

masts, school playing fields, car parking etc. If the enquiry is about environmental information, follow the guidance on the Department for Environment, Food and Rural Affairs (DEFRA) website.

Freedom of Information requests *must* be made in writing (including email) and should include the enquirer's name, correspondence address (email addresses are allowed) and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation (as referred to above), they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the School require further information in order to deal with your request, the School will request this further information directly from the individual making the request. Please note that the School do not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the School receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held and supplying any information that is held, except where exemptions apply. There is a time limit of 20 school days (i.e., excluding school holidays) for responding to the request.

Information

Provided all requirements are met for a valid request to be made, the School will provide the information that it holds (unless an exemption applies).

Holding information means information relating to the business of the school:

- That the school has created; or
- That the school has received from another body or person; or
- Held by another body on the school's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority (for example, the Local Authority), check whether they hold the information and if so, transfer the request to them. If this applies, the School will notify the enquirer that they do not hold the information and to whom they have transferred the request. The School will continue to answer any parts of the enquiry in respect of information it does hold.

When the School does not hold the information, it has *no duty to create or acquire it* just to answer the enquiry; although a reasonable search will be made before confirming whether the School has the information requested.

If the information requested is already in the public domain, for instance, through the Publication Scheme or on the School's website, the School will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the School (subject to any of the exemptions). This obligation is known as the school's *duty to confirm or deny* that it holds the information. However, the school does not have to confirm or deny if:

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

Vexatious Requests

There is no obligation on the Schools to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information and would require a substantial diversion of resources or would otherwise undermine the work of the school. However, this does not provide an excuse for bad records management.

In addition, the Schools do not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.

Fees

The School may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold. The threshold is currently £450 with staff costs calculated at a fixed rate of £25 per hour (therefore 18 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the school can only charge for the cost of informing the applicant whether the information is held and communicating the information to the applicant (e.g., photocopying, printing and postage costs).

When calculating costs/threshold, the School can take account of the staff costs/time in determining whether the information is held by the School, locating and retrieving the information and extracting the information from other documents. The School will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit (£450), the school can turn the request down, answer and charge a fee or answer and waive the fee.

If the School are going to charge, they will send the enquirer a fees notice. The School do not have to comply with the request until the fee has been paid. More details on fees can be found on the Information Commissioner's Office (ICO) website.

If planning to turn down a request for cost reasons or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the School by different people who appear to be acting together or as part of a campaign, the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

Time Limits

Compliance with a request must be prompt and within the time limit of 20 school days (this does not include the school holidays or weekends) or 60 working days if this is shorter. 'School' days is defined by the ICO as any day on which there is a session, and the pupils are in attendance. Failure to comply could result in a complaint by the requester to the ICO. The response time starts counting as the first day from the next working day after the request is received (so if a request was received on Monday 6th October the time limit would start from the next working day, the 7th October). Where the School has asked the enquirer for more information to enable it to answer, the 20 school days start time begins when this further information has been received.

If some information is exempt this will be detailed in the School's response.

If a qualified exemption applies and the School need more time to consider the public interest test, the School will reply in 20 school days stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a "reasonable" time.

Where the School has notified the enquirer that a charge is to be made, the time period stops until payment is received.

Third Party Data

Consultation of third parties may be required if their interests could be affected by release of the information requested and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights;
- The views of the third party may assist the School to determine if information is exempt from disclosure; or

- The views of the third party may assist the School to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document (e.g., Governing Body minutes) which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

Exemptions

The presumption of the Freedom of Information Act is that the School will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The School may refuse all/part of a request, if one of the following applies: -

1) There is an exemption to disclosure within the Act;
2) The information sought is not held;
3) The request is considered vexatious or repeated; or
4) The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are specialised in their application (such as national security) and would not usually be relevant to schools.

There are two general categories of exemptions:-

1) *Absolute*: where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest; and
2) *Qualified*: where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

Absolute Exemptions

There are eight absolute exemptions set out in the Act. However, the following are the only absolute exemptions which will apply to the School: -

- Information accessible to the enquirer by other means (for example, by way of the School's Publication Scheme);
- National Security/Court Records;
- Personal information (i.e., information which would be covered by the Data Protection Act);
- Information provided in confidence.

If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

Qualified Exemptions

If one of the below exemptions apply (i.e., a qualified disclosure), there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the School are: -

- Information requested is intended for future publication (and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published);
- Reasons of national security;
- Government/international relations;
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the School;
- Law enforcement (i.e., if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice);

- Release of the information would prejudice the ability of the School to carry out an effective audit of its accounts, resources and functions;
- For health and safety purposes;
- Information requested is environmental information;
- Information requested is subject to legal professional privilege; and
- For *commercial interest* reasons.

Where the potential exemption is a qualified exemption, the School will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it. In all cases, before writing to the enquirer, the person given responsibility by the School for dealing with the request will need to ensure that the case has been properly considered and that the reasons for refusal or public interest test refusal, are sound.

Refusal

If it is decided to refuse a request, the School will send a refusals notice, which must contain:

- The fact that the responsible person cannot provide the information asked for;
- Which exemption(s) apply;
- Why the exemption(s) apply to this enquiry (if it is not self-evident);
- Reasons for refusal; and
- The School's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld, and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

The School will get advice from their Data Protection Officer (DPO) prior to withholding data under an exemption or refusing the request in its entirety.

Section 2 – Freedom of Information Publication Scheme

This publication scheme follows a model approved by the Information Commissioners Office.

This scheme is not a list of individual publications but rather a description of the classes of types of information that we are committed to publishing. This list is not an exhaustive list of all of the types of information that we publish. We try to proactively publish as much information as we can where the information would have a wider public interest.

This scheme does not include information that we consider to be sensitive, such as personal information, information prevented from disclosure by law or information about security matters.

Classes of Information

There are six classes of information that we hold:

- Who we are and what we do
- What we spend and how we spend it
- What our priorities are and how we are doing
- How we make decisions
- Our policies and procedures
- The services we offer

Making Information Available

Information will generally be made available on the school website. Where it is not possible to include this information on the school website, the school will indicate how information can be obtained by other means and provide it by those means. This may be detailed in

response to a request or within the scheme itself. This will usually be by way of a paper copy.

In some exceptional circumstances, some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where we are legally required to translate any information, we shall do so.

Charges for Information Published Under This Scheme

The school may charge individuals for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at the minimum inconvenience and cost to the public. Charges made by the school for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on the website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by law.

Charges will be made to cover:

- Photocopying;
- Postage and packaging; and
- The costs directly incurred as a result of viewing information.

Single copies of information requested which are covered by the publication scheme will be provided free unless otherwise stated within the scheme. If the request involved a large amount of photocopying, printing or postage, then this may be at a cost. If this is the case we will let you know as well as let you know the cost before fulfilling your request.

How to Request Information

If you require a paper version of any of the documents within the scheme, please contact the school using the contact details below.

Telephone: 02086607500 or 02086605630

Email: office1@christchurch.croydon.sch.uk or office@purley.croydon.sch.uk

Address: Christ Church Primary School, Montpelier Rd, Purley CR8 2QE

Purley Nursery School, 58 Pampisford Road, Purley CR8 2NE

Please mark all correspondence *Publication Scheme Request* in order to help us process your request quickly. If the information you are looking for isn't available via the scheme, you can still contact the school to ask if we have this information.

The Publication Scheme

Who We Are and What We Do	**Description**

Information relating to the Governing Body	Information contained in official governing body documents including the governor's annual report:- · Who is who · Basis of governors appointment · The manner in which the governing body is constituted · Category of the school · A statement on progress in implementing the action plan drawn up following an inspection · Agreed minutes from governors board and committee meetings · A financial statement – including gifts made to the school and amounts paid to the governors for expenses · Information about the implementation of the governing body's policy on pupils with special educational needs and any changes to the policy during the last year · A description of arrangements for the admission of pupils with disabilities, including details of the steps to prevent disabled students being treated less favourably than other pupils, details of existing facilities to assist access to the school by pupils with disabilities, the accessibility plan covering future policies for increasing access by those with disabilities to the school · A statement of policy on whole staff development identifying how teacher's professional development impacts on teaching and learning.

	· Number of pupils on roll and rates of pupils authorised and unauthorised absence · National curriculum assessment results for appropriate key stages with national summary figures · Instruments of government, including the date it takes effect · The term of office of each category of governor if it lasts less than 4 years and the name of anybody entitled to appoint any category of governor.
School prospectus	· The name, address, website and telephone number of the school and the type of school · The name of the school Headteacher · The school's staffing structure · Information about the schools policy on providing for pupils with special educational needs · Statement on the schools aims and values · Information on the school policy on admissions · School term dates, times and attendance · Uniform · Number of pupils on roll and rates of student absence · Details of any affiliations with a particular religion or religious denomination, the religious education and collective worship and the alternative provision for these pupils.

What We Spend and How We Spend It	Description
Financial statement for the current and previous financial year	Relating to projected and actual income and expenditure, procurement, contracts and financial audit. Includes budget plans, financial statements and financial audit reports.
Details of expenditure	Sets out details of items of expenditure over £5,000 including the cost, name of supplier and information about the transaction.
Procurement and contracts	Details of the procurement and contracts the school has entered into or details relating to the organisation who has carried out this process on the schools behalf (for example the local authority).
Pay policy	A copy of the pay policy that the school uses to govern staff pay.
Allowances	Details of allowances and expenses that can be incurred by staff and governors.
Pupil Premium	How the school uses pupil premium.
Utilities and school running expenditure	Details of the schools overheads and running costs.

What Our Priorities Are and How We Are Doing	Description
Ofsted report	A published report of the outcome of our latest Ofsted inspection.
Performance management Policy	Statement of procedures adopted by the governing body relating to the performance management of staff and the

	annual report of the Headteacher on the effectiveness of appraisal procedures.
Charging and remissions policies	A statement of the school's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted, for example school publication, music tuition, trips.
Health and Safety Policy and Risk Assessment	Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy.
Staff Conduct, Discipline and Grievance	Statement of procedure for regulating conduct and discipline of school staff and procedures by which staff may seek redress for grievance.

How We Make Decisions	**Description**
Admissions Policy/ Decisions (not individual)	This does not include individual decisions. This is a statement of our policy with regards to admissions and how we make decisions regarding admissions.

Our policies and procedures	**Description**
Home-School Agreement	Written statements of the schools aims and values, the schools responsibilities, the parental responsibilities the schools expectations of its pupils for example homework arrangements.

Curriculum Policy	Statement on following the national curriculum subjects, including any syllabus used by the school.
Complaints Policy	Statement of procedures for dealing with complaints.
Equality and Diversity Policy	Statement on ensuring that the school follows and promotes equality and diversity.
Child protection and safeguarding policy	Statement of policy for safeguarding and promoting welfare of pupils at the school.
Relationships and Sex Education Policy	Statement of policy with regard to sex and relationship education.
Inclusion Policy	Information about the school's policy on providing for pupils with special educational needs.
Behaviour Policy	Statement of general principles on behaviour and discipline and of measures taken by the Headteacher to prevent bullying.
Collective Worship	Statement of arrangements for the required daily act of collective worship.

Lists and Registers	**Description**
Curriculum Circulars and Statutory instruments	Any statutory instruments, departmental circulars and administrative memoranda sent by the Department of Education to the Headteacher or governing body relating to the curriculum.
Asset Register	A record of major physical assets owned by the school (e.g., computers, furniture, equipment). This is available on request.
CCTV – Details of the locations of any overt CCTV surveillance cameras	Information is available in hard copy upon request

operated by us of on our behalf	
Disclosure Log (FOI Requests) (Appendix 1)	A summary of FOI requests received and how the school responded. Includes date, topic of request and summary of response.
Any information you are currently legally required to hold in publicly available registers	Including staffing structure (names/roles of senior leadership) and governors.

The services we offer	**Description**
Extra-curricular activities and out of school clubs	Details of these are contained in our newsletter, leaflets, new intake packs

Internal Review

The requester has the right to ask for an internal review if they are dissatisfied with the handling of a request.

Internal review requests should be made within 40 working days of the initial response. This deadline should be communicated to the requester in that response. We are not obliged to provide a review if it is requested after more than 40 working days.

Requests for internal review must make clear why they are dissatisfied with the original decision, detailing why they feel that the School has not complied with Freedom of Information Law.

Complaints and/or Appeals

Any written (including email) expression of dissatisfaction should be handled through the School's existing complaints procedure. Wherever practicable the review should be handled by someone not involved in the original decision.

The Governing Body should set and publish a target time for determining complaints and information on the success rate in meeting the target. The school should maintain records of all complaints and their outcome.

If the outcome is that the School's original decision or action is upheld, then the applicant can appeal to the Information Commissioner. The appeal can be made via their website or in writing to:

Customer Contact:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

SK9 5AF

Appendix 1: FOI Disclosure Log[SH4]

Guidance note: This is to record a summary of what has been provided as part of a FOI request that has been complied with. It is considered best practice by the ICO, especially if you receive frequent or similar FOI requests. It also assists with improving transparency and reducing administrative work by pre-empting repeat questions.

The log should be clear and non-technical. We would recommend that this is accessible and published on the school website. The school should avoid disclosing personal or sensitive information (i.e., not detailing requesters name and contact information). The log should be kept up to date.

Request number/ ID	Date of Request	Summary of Request	Date of Response	Summary of Response	Exemptions Applied (if any)	Link to information (if applicable)

Example: FOI2025/01	*01/01/2025*	*Number of exclusions in 2023/24 by year group*	*20/01/2025*	*Provided figures broken down by year*	*None*	*N/A*

se your organisation's contacts or address book. This helps to stop emails being sent to the wrong address.

Don't:

- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- Turn off any email security measures that your IT team has put in place or recommended.