



ELTHAM

**CHURCH OF ENGLAND
PRIMARY SCHOOL**

SINCE 1814

Eltham C of E SCHOOL

DATA PROTECTION (GDPR) POLICY

CREATED BY: AGAS DATA PROTECTION OFFICER

REVIEWED BY: GOVERNING BODY

LAST REVIEW: NOVEMBER 2022

NEXT REVIEW DATE: SEPTEMBER 2025

**This policy complies with Data Protection Act 2018, and with the requirements of the
General Data Protection Regulation from 25 May 2018**

This policy and content is the property of Eltham C of E School and no part of it may be used or reproduced in part or otherwise without the permission of the Headteacher. The information contained herein is to be considered to be sensitive and should be kept confidential at all times.

1. STATEMENT OF INTENT

Eltham C of E School (the "**School**") collects and uses Personal Data about its staff members (including governors), pupils, parents and other individuals who come into contact with the School in accordance with its legal obligations under the General Data Protection Regulation ("**GDPR**") and the Data Protection Act 2018 ("**DPA**"). Personal Data is gathered in order to enable the School to provide education and other associated functions. The School will ensure that any Personal Data is processed fairly as directed by the principles of data protection and as guided by best practice from the Information Commissioner's Office ("**ICO**").

The School is the Data Controller for the purpose of the GDPR and is registered with the ICO detailing the information held and its use.

2. FAIR PROCESSING NOTICES

Schools also have a duty to issue a Fair Processing Notice ("**FPN**") to all pupils/parents. The FPN summarises the information held on pupils/parents; why such information is held; how information is processed; the rights of pupils/parents in relation to information (such as the ability to withdraw consent); the other parties to whom information may be passed on; and the period for which information will be held for.

3. PURPOSE

The purpose of this policy is to ensure that Personal Data is dealt with by the School correctly and securely and that the School complies with data protection laws and professional regulations (including but not limited to the GDPR and DPA) and protects the data rights of its staff members (including governors), pupils, parents and other individuals who come to contact with the School.

4. SCOPE

This policy will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and will apply to information contained in any form, including for example email, spoken information, or handwritten or printed documents.

This policy covers all staff members (at all levels and grades) involved with the collection, processing and disclosure of Personal Data and all staff members (including governors) will be aware of their duties and responsibilities by adhering to this policy and the School will offer continued training to assist with GDPR and DPA compliance.

This policy will be reviewed as it is deemed appropriate, but no less frequently than every year to ensure relevance, compliance and best practice. The policy review will be undertaken by (the "**Headteacher**") or a nominated representative.

5. DEFINITIONS

Data Controller	Is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Subject	Is an individual who is the subject of Personal Data.
Personal Data	Is data which relate to a living individual who can be identified (a) from those data; or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller.

Special Categories of Personal Data	Is information concerning the Data Subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.
--	---

6. PRINCIPLES

The GDPR is an EU regulation intending to combine and strengthen data protection within the European Union ("EU"). The GDPR covers all countries that hold or process Personal Data belonging to EU citizens, whether they are located in the EU or not. The GDPR establishes seven enforceable principles that must be adhered to all times when processing Personal Data, as follows:

Seven Principles	
Lawfulness, fairness and transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject (being individuals).
Purpose limitation	Personal Data shall be collected to specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. More information regarding legitimate purposes for further processing can be found in Article 89(1).
Data minimisation	Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate data (having regard to the purposes for which they are processed) is erased or rectified without delay.
Storage limitation	Personal Data shall be kept in a form which permits identification of the Data Subjects (for no longer than is necessary for the purposes for which the Personal Data are processed), and Personal Data may be kept for no longer periods than is necessary for the purposes for which the personal data is being processed. More information regarding when personal information is permitted to be stored beyond this can be found in Article 89(1).
Integrity and confidentiality	Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The Data Controller shall be responsible for, and be able to demonstrate compliance with, the GDPR.

7. GENERAL STATEMENT

The School is committed to maintaining the above seven principles at all times. Therefore the School will:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, and why and with whom the information was shared with;
- Check the quality and the accuracy of the information it holds;
- Ensure that information is not retained for longer periods than is necessary;
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely;

- Ensure that clear and robust safeguards are in place to protect Personal Data from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to Personal Data, known as Subject Access Requests; and
- Ensure that staff members are aware of and understand the School policies and procedures.

8. NEW RIGHTS POST GDPR

Data Subject Rights	
Right to be informed	Individuals have the right to be informed about the collection of their data, including the purpose of processing, retention periods, and who their data will be shared with.
Right of access	Individuals have the right to obtain confirmation that their personal data is being processed, and the purpose of the processing, as well as a copy of their personal data and other supplementary information. If requested, the data must be available in a commonly used electronic format.
Right to rectification	If the personal data held is inaccurate or incomplete the individual has the right to ask for the information to be corrected.
Right to erasure	Individuals have the right to have their personal data erased under certain circumstances; such as if it is no longer relevant to the purpose of processing or the data subject is withdrawing consent.
Right to restrict processing	Individuals have the right to request that processing of their personal data is restricted or suppressed under certain circumstances, such as if they are contesting the accuracy of information or it has been processed unlawfully.
Right data portability	Individuals have the right to obtain and reuse their personal data for their own purposes, and are able to transfer their personal data electronically in a safe and secure way without hindrance to usability.
Right to object	Individuals have the right to object to profiling, processing based on legitimate interests, direct marketing, and processing for purposes of research and statistics.
Automated decision making and profiling	Individuals have the right to challenge decisions made by automated means or profiling.

9. SUBJECT ACCESS REQUESTS ("SAR")

Right of access to information

Under the GDPR any individual has the right to make a request access the Personal Data held about them, so that individuals are aware of such information, why such information is held about them and to verify the lawfulness of the processing of such information.

Actioning a SAR

Below is the process detailing how the School will handle a SAR:

1. **Request:** Requests to access Personal Data must be made in writing using the SAR Pro Forma and the more information that is provided on the SAR Pro Forma, the easier it will be for the School to locate the relevant Personal Data. The SAR Pro Forma can be submitted by post, addressed or electronically for the attention of the School's Data Protection Lead details of which are found in the contact section 12.
2. **Further Information:** If the initial request for SAR does not clearly identify the information required, then further enquiries will be made by the School.
3. **Proof of Identity:** The identity of the requestor for SAR must be established before disclosure of any information is made by the School, and checks will also be carried out by the School regarding proof of relationship to the pupil. The requestor for SAR can evidence their identity by submitting the following:
 - Passport;
 - Driving licence;
 - Utility bills with the current address;
 - Birth/ marriage certificate;
 - P45/P60; or
 - Credit card or mortgage statement.

This list is not an exhaustive list.

4. **Children and SAR:** Any individual has the right of access to information held about them and children have the same rights as adults over their Personal Data in relation to right to access their Personal Data. However with children, this right is dependent upon their capacity to understand (normally aged [13] or above) and the nature of the request. Personal Data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of SAR's. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent. Therefore, most SAR's from parents of pupils at this School will not be granted without the express permission of the pupil. Parents at this School do not have an automatic right to access their child's educational record. The School will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the ICO.
5. **Charges:** The school will provide the information requested free of charge.
6. **Excessive/unfounded Requests:** The School may charge a reasonable fee if the request for information is manifestly excessive or unfounded, particularly if the request is repetitive. The fee charged will be determined on the basis of the administrative costs of complying with the request and therefore the level of the fee will vary depending on the remit of the request and the administrative costs incurred. The School will need to provide evidence to the requestor on how the request for information is manifestly excessive or unfounded.
7. **Unwarranted Requests:** The School may refuse to respond to unwarranted requests for information. The School will explain the reason of refusal to the requestor, inform the requestor of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at least within a month.
8. **Electronic requests:** The right to request information may be submitted electronically to the School's Data Protection Lead using the SAR Pro Forma form, unless otherwise requested by the individual. Also, the requestor may make a SAR using any Facebook page or Twitter account that the School has, other social-media sites to which the School subscribes, or via third party websites. The School cannot insist on the use of a particular means of delivery for a SAR.

9. Time to Respond: The response time for SAR for all or part of the pupil's educational record, once officially received, is fifteen (15) school days. If the SAR does not relate to the pupil's educational record, the School will respond to a SAR without undue delay and in any event within one (1) month of receipt of the request. The School may extend the deadline to respond to a SAR by up to two (2) months (so up to three (3) months in total) where the SAR is particularly complex or numerous and if this is the case the School will contact the requestor within one (1) month of making the request and inform he or she why an extension is necessary.
10. Right to Withhold Personal Data: The School has the right to withhold the disclosure of Personal Data upon a SAR if disclosure would adversely affect the rights and freedoms of others.
11. The GDPR allows exemptions as to the provision of some information; therefore all information subject to a SAR will be reviewed prior to disclosure.
12. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.
13. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the pupil is at risk of abuse, or information relating to court proceedings.
14. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
15. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then such information should be retyped.
16. Information can be provided at the School with a member of staff on hand to help and explain matters if requested, or provided at a face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

10. COMPLAINTS

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

11. DATA BREACH MANAGEMENT PROCEDURE

Appropriate measures are taken against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data by the school. This procedure will be followed in the event of a data security breach, examples of which are:

- Loss or theft of data or equipment on which data is stored on school
- premises or outside
- Inappropriate access controls allowing unauthorised use

- Equipment failure
- Human error - correspondence with personal data sent to the wrong email address
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit from the school

The school will follow the following steps if a data security or potential data security breach occurs:

Detection

When a member of staff becomes aware that a breach or potential breach has occurred, they must notify the DPO as soon as possible.

Containment and recovery

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- Where appropriate, inform the police
- Assess whether the breach should be reported to the ICO
- Notify the ICO within 72 hours of breach being detected if breach is identified as serious

Assessment of ongoing risk

The following points are also likely to be helpful in making this assessment:

- What type of data is involved – staff or pupil sensitive personal data
- Where personal data has been lost or stolen, are there any protections in place such as encryption?
- How many staff and/or pupil's personal data are affected by the breach?
- What harm can be done to these individuals – risks to physical safety, reputation etc.

Notification of breach

The DPO will arrange for those affected by the breach to be notified as soon as practically possible.

Evaluation and response

In the event of a breach, the DPO will complete an investigation as to the causes of the breach and also evaluate the effectiveness of the school's response to it. This will be reported to a Committee of the Governing Body and where necessary, the school will update its policies and procedures accordingly. The school will maintain a log of breaches, specifying the nature of the incident and the response taken.

12. PRIVACY NOTICES

This policy has three separate appendices, which are:

1. Appendix 1: Privacy Notice - How we use pupil Information
2. Appendix 2: Privacy Notice – How we use Employee Information
3. Appendix 3: Privacy Notice – How we use Parent/Carer Information

13. CONTACTS

If you have any enquires in relation to this policy, please contact the Headteacher who will also act as the point of contact for any SAR's.

Data Protection Lead ("DPL"): sao1@elthamce.greenwich.sch.uk

Email: sao1@elthamce.greenwich.sch.uk

Further advice and information is also available from the ICO at <https://ico.org.uk/> or telephone the ICO helpline on 0303 123 1113 (UK) or if you're calling from outside of the UK on 441625545700.

APPENDIX I: PRIVACY NOTICE – HOW WE USE PUPIL INFORMATION

This privacy notice explains how and why we collect pupils' Personal Data, what we do with such data and the rights that parents and pupils have in relation to the use of their data.

1. DATA PROTECTION OFFICER ("DPO")

The AGAS Data Protection Officer will:

- Inform and advise the School and its staff members about their obligations to comply with the GDPR and other data protection laws.
- Monitor the School's compliance with the GDPR and other data protection laws, including managing internal data protection activities, conducting internal audits and providing the required training to staff members.
- Report to the highest level of management in the School, which is the Headteacher.

2. DATA PROTECTION LEAD ("DPL")

The DPL for the School is Mr Matthew Wills The DPL will:

- Ensure the school is in line with GDPR compliance and knows its responsibilities as the Data Controller.
- To liaise with the DPO in accordance to GDPR regulations and Data Breaches.

3. CATEGORIES OF PERSONAL DATA HELD BY THE SCHOOL ABOUT ITS PUPILS

The School may collect, use, store or share (where appropriate) the following categories of data about its pupils:

- Name.
- Unique pupil number.
- Contact details.
- Contact preferences.
- Date of birth.
- Identification documents.
- Results of internal assessments and externally set tests.
- Pupil and circular records,
- Pupil characteristics such as:
 - Ethnic background.
 - Language.
 - Nationality.
 - Country of birth.
 - Eligibility for free school meals.
 - Special educational needs.
 - Medical conditions, including physical and mental health.
- Behaviour records, such as exclusion information (if relevant).
- Attendance information, such as lessons attended, number of absences and absence reasons.
- Safeguarding information.
- Details of any support received, including care packages, plans and support providers.

- Data received about pupils from other organisations, including other schools, local authorities and the Department for Education.

Whilst the majority of pupil information you provide to the School is mandatory, some of it is provided to the School on a voluntary basis. In order to comply with the GDPR, the School will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. Where appropriate, the School will ask parents for consent to process Personal Data where there is no other lawful basis for processing it, for example where the School wishes to use photos or images of pupils on its website or on social media to promote the School activities or if the School wants to ask your permission to use your information for marketing purposes. Parents / pupils may withdraw consent at any time.

Biometric Data

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements. Schools and colleges that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018. In accordance with this policy the school does not currently process any biometric data.

CCTV

The School also uses CCTV cameras around the School site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or to investigate other issues. CCTV footage involving pupils will only be processed to the extent that it is lawful to do so. Please see our Management and Retention of Records Policy.

The School collects information about pupils when they join the School and continues to update such information during their time on the roll and as and when new information is acquired.

4. WHY WE COLLECT AND USE PUPIL DATA

The School collects and uses pupil data to:

- Decide who to admit to the School.
- Maintain a waiting list.
- Support pupil learning.
- Monitor and report on pupil learning and progress.
- Provide appropriate pastoral care.
- Protect pupil welfare and others in the School.
- Assess the quality of the School's services.
- Comply with the law regarding data sharing.
- Provide a safe and orderly running of the School.
- Promote the School.
- Communicate with parents/carers.
- Respond to investigations from our regulators or to respond to complaints raised by our stakeholders.
- Use in connection with any legal proceedings threatened or commenced against the School.

5. LEGAL BASIS FOR USING PUPIL DATA

The School will collect and use pupils' data under the following lawful bases:

- a. Where the School has obtained the consent of the Data Subject for processing. Where the School has obtained the consent of the Data Subject (pupil) to use pupils' Personal Data, this consent can be withdrawn at any time. The School will make this process clear when consent is sought and will explain in detail how consent can be withdrawn.
- b. Where it is necessary for the School to comply with a legal obligation.
- c. To protect the vital interests of the Data Subject or another person.

- d. Where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

Where the Personal Data the School collects about its pupils is a Special Categories of Personal Data (as defined in section 5 of the Data Protection Policy), the School must meet one of the following criteria:

- a. Have the pupils' explicit consent (unless reliance on consent is prohibited by the EU or Member State law).
- b. It is necessary to protect the vital interests of the Data Subject or of another natural person.
- c. It is necessary for reasons of substantial public interest.
- d. Have obligations or rights under any other law.

6. STORING PUPIL DATA

The School keeps Personal Data about pupils while they are attending the School. The School may also keep Personal Data beyond the attendance of its pupils, in order to comply with its legal obligations. A significant amount of Personal Data is stored electronically, for example, on the School Information Management System (SIMs) Some Personal Data may also be stored in hard copy format. Personal Data stored electronically may be saved on a cloud-based system which may be hosted in a different country, that is, within the EU borders only (unless there is a legitimate reason to store the Personal Data outside of the EU or consent of the Data Subject has been obtained). Personal Data may be transferred to other countries within the EU borders only (unless there is a legitimate reason to store the Personal Data outside of the EU or consent of the Data Subject has been obtained) if, for example, the School is arranging a school trip to a different country. Appropriate steps will be taken to keep Personal Data secure. The School's Management and Retention of Records Policy sets out how long the School keeps information about its pupils. Copies of all policies can be found on the School website.

7. DATA SHARING

The School does not share Personal Data about its pupils with any third party without consent, unless the law or the School policies allow the School to do so. Where it is legally required, or necessary (and it complies with the data protection law), the School may share Personal Data about its pupils with:

- Parents / carers (as defined in the Education Act 1996).
- Schools that pupils attend after leaving the School.
- The local authority, that is, Greenwich to meet legal obligations to share certain information with it, such as safeguarding concerns and exclusions).
- A pupil's home local authority (if different).
- The Department for Education (DFE)(Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013). To find out more about the data collection requirements placed on the School by the Department for Education (for example; via the School census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>
- The School governors.
- Educators and examining bodies.
- The School regulator (Ofsted).
- The Police and law enforcement agencies.
- NHS health professionals including the School nurse and educational psychologists.
- Education Welfare Officers.
- Courts and tribunals (if ordered to do so).
- The National College for Teaching and Learning.
- The Joint Council for Qualifications.
- Prevent teams in accordance with the Prevent Duty on schools.
- Other schools, for example, if the School is negotiating a managed move and the School has obtained pupil consent to share information in these circumstances.
- Diocesan Officers at the Southwark Diocesan Board of Education for the purposes of receiving educational support.
- The School chaplain.
- The School's HR providers, for example, if the School is seeking HR advice and a pupil is involved in an issue.
- Legal advisors.

- Insurance providers / the Risk Protection Arrangement.

This list is not an exhaustive list.

Some of the above organisations may also be Data Controllers in their own right in which case we will be jointly controllers of pupil Personal Data and may be jointly liable in the event of any data breaches. In the event that the School shares Personal Data about pupils with third parties, the School will provide the minimum amount of Personal Data necessary to fulfil the purpose for which the School is required to share the data.

8. NATIONAL PUPIL DATABASE ("NPD")

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

The School is required by law, to provide information about its pupils to the DFE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information the School shares with the DFE, for the purpose of data collections, go to: <https://www.gov.uk/education/data-collection-and-censuses-for-schools>. To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>. The database is held electronically so that it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The DFE may share information about the School's pupils from the NPD with other third parties who promote the education or well-being of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

Such third parties must agree to strict terms and conditions about how they will use the data.

The DFE has robust processes in place to ensure the confidentiality of the School data is maintained and there are stringent controls in place regarding access and use of the data.

Decisions on whether the DFE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data.
- The purpose for which the data is required.
- The level and sensitivity of data requested.
- The arrangements in place to store and handle the data.

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

For more information about the department's data sharing process, please visit:

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

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact the DFE, please visit the following website: <https://www.gov.uk/contact-dfe-with-any-further-questions-about-the-npd>.

9. REQUESTING ACCESS TO YOUR PERSONAL DATA

Under the GDPR, parents and pupils have the right to request access to information about them that the School holds, known as a SAR. Where a child does not have the maturity to make their own SAR for Personal Data (usually under the age of 12) or where the child has provided consent, parents may do so on their behalf in a primary school setting. Parents also have the right to make a SAR with respect to any Personal Data the School holds about them. To make a request for your child's personal data, or be given access to your child's educational record, please contact the DPO or School Data Protection Lead although any written request for personal data will be treated as a SAR.

If you make a SAR, and if the School holds information about you or your child, the School will:

- Give you a description of the information.
- Tell you why the School is holding and processing such information and how long the School will keep the information.
- Explain to you where the School got the information from (that is, if such information is not from you or your child).
- Tell you with who such information has been shared with.
- Let you know whether any automated decision-making is being applied to the data and any consequences of this.

Give you a copy of the information in intelligible form.

As the School has limited staff resources outside of term time, we encourage parents / pupils to submit SAR during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible.

Details about making a SAR can be found in section 9 of the Data Protection Policy.

10. OTHER RIGHTS

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

- Object to processing of Personal Data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means (by a computer or machine, rather than a person).
- In certain circumstances, have inaccurate Personal Data rectified, blocked, erased or destroyed.
- Claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of the above rights, please contact the School DPO.

11. COMPLAINTS

The School takes any complaints about its collection and use of Personal Data very seriously. If you have a concern about the way we are collecting or using your child's or your Personal Data, you should raise your concern with us in the first instance. To make a complaint, please contact our DPO. Alternatively, you can make a complaint to the ICO:

- [Report a concern online at: https://ico.org.uk/make-a-complaint/](https://ico.org.uk/make-a-complaint/)
- [Call: 0303 123 1113 \(local rate\) or 01625 545 745 \(if you prefer to use a national rate number\)](tel:03031231113)
- [Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF](mailto:complaints@ico.org.uk)

12. CONTACT US

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

- AGAS Data Protection Officer – Dataprotectionofficer@koinoniafederation.com

CHANGES TO THIS PRIVACY NOTICE

We the School reserves the right to update this privacy notice at any time, and we the School will provide you with a new privacy notice when we make any substantial updates are made. We the School may also notify you in other ways from time to time about the processing of your pupil personal information.

APPENDIX 2: PRIVACY NOTICE - HOW WE USE EMPLOYEE INFORMATION

1. GENERAL

This privacy notice explains how and why we collect and use Personal Data about our members of staff (hereafter referred to as "you" or "your") before, during and after your working relationship with the School, what we do with such Personal Data and what rights you have in relation to the use of such Personal Data, that is, in accordance with the GDPR.

2. APPLICATION OF THIS POLICY

The School is responsible for deciding how it holds and uses Personal Data about you. Accordingly, the School is required under the GDPR to notify you of the information contained in this privacy notice. Once notified, it is your responsibility to read this policy, together with any other privacy notice the School may provide on specific occasions and when the School is collecting Personal Data about you. This privacy notice applies to all current and former employees, workers and contractors of the School. This privacy notice does not form part of any contract of employment or other type of contract to provide services. The School may, at any time, in its absolute discretion, update or amend this privacy notice and notify you forthwith of such changes.

3. DATA PROTECTION OFFICER ("DPO")

The AGAS Data Protection Officer will:

- Inform and advise the School and its staff members about their obligations to comply with the GDPR and other data protection laws.
- Monitor the School's compliance with the GDPR and other data protection laws, including managing internal data protection activities, conducting internal audits and providing the required training to staff members.
- Report to the highest level of management in the School, which is the Headteacher.

4. DATA PROTECTION LEAD ("DPL")

The DPL for the School is Matthew Wills. The DPL will:

- Ensure the school is in line with GDPR compliance and knows its responsibilities as the Data Controller.
- To liaise with the DPO in accordance to GDPR regulations and Data Breaches.

5. DATA PROTECTION PRINCIPLES

The School will comply with the GDPR. The GDPR stipulates that the Personal Data the School holds about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid, specified, explicit and legitimate purposes that that the School has clearly explained to you and is not used in any way that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which such Personal Data is processed.
- Accurate and kept up to date (where necessary).
- Kept only as long as necessary for the purposes for which the Personal Data is being processed.

- Kept securely.

6. WHY WE COLLECT PERSONAL DATA ABOUT YOU

The School processes Personal Data about you for employment purposes to assist in the running of the School and/or to enable you to be paid. The collection of your Personal Data will benefit both national and local users by:


- Improving the management of workforce data across schools.
- Enabling development of a comprehensive picture of the workforce and how it is deployed.
- Informing the development of recruitment and retention policies.
- Allowing better financial modelling and planning.

7. CATEGORIES OF PERSONAL DATA HELD BY THE SCHOOL ABOUT YOU

Personal Data means any information about an individual from which that individual can be identified from such data. Personal Data does not include data where the identity of the individual has been removed (anonymous data).

The School may collect, store, use and share (where appropriate) the following categories of Personal Data about you:

- Personal contact details such as name, title, address, telephone number and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance Number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Teacher Reference Number.
- Employment start date at the School.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of pre-vetting recruitment and identity checks (including, where appropriate, information about your employment history, Standard or Enhanced Disclosure and Barring Service Checks, Barred Lists Checks, prohibition checks /section 128 checks and disqualification checks, for example under the Childcare (Disqualification) Regulations 2009 and any further checks that are required if you have lived or worked outside the UK), your nationality and right to work documentation, references and other information included in a CV, application form or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Details of approved absences (career breaks, parental leave, study leave etc.).
- Compensation history.
- Performance information.
- Photographs.
- Disciplinary and grievance information, including warnings and complaints issued to you.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.

 *This list is not exhaustive*

The School may also collect, store, use and share (where appropriate) the following Special Categories of Personal Data about you:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership/activities.

- Information about your health, including any medical condition (physical or mental health), health and sickness records.
- Genetic information and biometric data.
- Information about your criminal record.

8. HOW IS YOUR PERSONAL DATA COLLECTED

The School collects Personal Data about employees, workers and contactors through the application and recruitment process, that is, either directly from candidates or sometimes from an employment agency or background check providers. The School may also collect Personal Data from third parties including former employers or the Local Authority. The School will also collect additional Personal Data in the course of job related activities throughout the period of you working for the School.

9. LEGAL BASIS FOR USING YOUR PERSONAL DATA

The School will only use your Personal Data when the law allows the School to do so. Most commonly, the School will use your Personal Data in the following circumstances:

- Where the School has obtained your consent for the processing of your Personal Data and this consent can be withdrawn at any time. The School will make this process clear when consent is sought and will explain in detail how consent can be withdrawn.
- Where the School needs to perform the contract of employment it has entered into with you.
- Where the School needs to comply with a legal obligation.

The School may also use your Personal Data in the following circumstances:

- Where the School needs to protect your vital interests (or someone else's vital interests)
- Where it is necessary in the public interest or for official purposes.
- Having obligations or rights under any other law.

10. SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL DATA

The situations in which the School will process your Personal Data are listed below, as follows:

- Making a decision about your recruitment or appointment.
- Determining the terms and conditions on which you work for the School.
- Checking that you are legally entitled to work in the United Kingdom.
- Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working in specific positions via the Teacher Services Online platform
- To maintain the School's single central record and to comply with the School's general safeguarding obligations.
- To provide information on the School website about our employees.
- Where appropriate, to disclose certain information in the School's accounts in accordance with the accounts direction.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Liaising with your pension provider.
- Administering the employment contract the School has entered into with you.
- In order to operate as a school, which may involve the School sharing certain information about its staff with its stakeholders or processing correspondence or other documents, audits or reports which contain your Personal Data.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Responding to complaints or investigations from the School's stakeholders or regulators.

- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of the working relationship between the School and you.
- Providing references to prospective employers.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of the School information and communication systems to ensure compliance with the School's IT policies.
- To ensure network and information security, including preventing unauthorised access to the School computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- In connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with a school conversion.
- To maintain and promote equality in the workplace.
- To comply with requirements of the Southwark Diocesan Board of Education to share Personal Data about employees to the extent that they require it to fulfil their functions.
- To receive advice from external advisors and consultants.
- In appropriate circumstances to liaise with regulatory bodies, such as the NCTL, the Department for Education (DFE), the Disclosure and Barring Service (DBS) and the Local Authority about your suitability to work in a school or in connection with other regulatory matters.

 *This list is not exhaustive.*

Some of the above grounds for processing will overlap and there may be several grounds which justify the School's use of your Personal Data.

The School also uses CCTV cameras around the School site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or investigate other issues. CCTV footage involving staff will only be processed to the extent that it is lawful to do so. Please see the School's Management and Retention of Records Policy for more details.

IF YOU FAIL TO PROVIDE PERSONAL DATA

If you fail to provide certain information when requested, the School may not be able to perform the contract it has entered into with you (such as paying you or providing a benefit), or the School may be prevented from complying with its legal obligations (such as to ensure the health and safety of its workers) or may be unable to discharge its obligations which may be in the public interest or for official purposes.

CHANGE OF PURPOSE

The School will only use your Personal Data for the purposes for which it was collected, unless the School reasonably considers that it needs to use your Personal Data for another reason and that reason is compatible with the original purpose. If the School needs to use your Personal Data for an unrelated purpose, the School will notify you and will explain the legal basis which allows the School to do so. Please note that the School may process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

II. HOW WE USE PARTICULARLY SPECIAL CATEGORIES OF PERSONAL DATA

Where the School collects "Special Categories of Personal Data" (as defined in section 5 of the Data Protection Policy) about you, the School will ensure higher levels of data protection. The School may process Special Categories of Personal Data in the following circumstances:

- In limited circumstances, with your explicit consent (unless reliance on consent is prohibited by the EU or Member State law).

- Where the School needs to carry out its legal obligations and in line with its Data Protection Policy.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to the School's occupational pension scheme.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Where it is necessary to protect your interests (or someone else's interests) and you're not capable of giving your consent or where you have already made the information public.
- Where the School has obligations or rights under any other law.

THE SCHOOL AND ITS OBLIGATIONS AS AN EMPLOYER

The School will use your particularly Special Categories of Personal Data in the following ways and the School will:

- Use information relating to leaves of absence including the reasons for the leave, which may include sickness absence or family-related leave or sabbaticals, to comply with employment and other laws.
- Use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to comply with the Equality Act 2010, to monitor and manage sickness absence and to administer benefits.
- Use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- Use trade union membership information to pay trade union subscriptions, register the status of a protected employee and to comply with employment law obligations.
- As the School is a Church of England school, the School will hold information about the religious beliefs of some employees so that we can assess their suitability to hold certain posts.

DOES THE SCHOOL NEED YOUR CONSENT

The School does not need your consent if it's using your Special Categories of Personal Data in accordance with its written policy where processing is necessary:

- To carry out its legal obligations or to exercise specific rights in the field of employment law;
- For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- For reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and the School provides for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

In other circumstances, the School may approach you for your written consent to allow the School to process Special Categories of Personal Data. If the School does so, it will provide you with full details of the information that it would like and the reason why the School needs such information, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract of employment with the School that you agree to any request for consent.

12. INFORMATION ABOUT CRIMINAL CONVICTIONS

The School will only use information relating to criminal convictions where the law allows the processing of such information. This will usually be where such processing is necessary for the School to carry out its legal obligations and provided that the School do so in line with its Data Protection Policy or Safeguarding Policy. Less commonly, the School may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. The School envisages that it will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of its recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with the School.

The School will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so. Where appropriate, the School will collect information about criminal convictions as part of the recruitment process or the School may be notified of such information directly by you in the course of you working for the School.

13. AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. The School is allowed to use automated decision-making in the following circumstances:

- a) Where the School has notified you of the decision and given you 21 days to request reconsideration.
- b) Where it is necessary to meet the School's obligations under your employment contract and ensure that appropriate measures are in place to safeguard your rights.
- c) In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

14. STORING YOUR DATA

Please see the School's Management and Retention of Records Policy.

15. DATA SHARING

The School does not share your Personal Data with third parties, including third-party service providers and other organisations (including contractors and designated agents) without your consent, unless the law or the School policies allow the School to do so, to administer the working relationship with you or it is needed in the public interest or for official purposes. In particular, where it is legally required or necessary (and it complies with the GDPR), the School may share your Personal Data with organisations including, but not limited to, the following:

- The Local Authority, that is, Greenwich.
- The DFE (on a statutory basis). To find out more about the data collection requirements placed on the School by the DFE (for example; via the School census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>
- The Education & Skills Funding Agency.
- The Southwark Diocesan Board of Education.
- The Disclosure and Barring Service.
- The Teaching Regulation Agency.
- The Teachers' Pension Service.
- The Local Government Pension Scheme which is administered by the School's external HR provider.
- The School's external payroll provider.
- The School's IT Provider.
- HMRC.
- The Police or other law enforcement agencies.
- The School's legal advisors.

- Insurance providers / Risk Protection Arrangement.

The School requires third parties to respect the security of your Personal Data and to treat it in accordance with the law. Some of the organisations referred to above are joint Data Controllers. This means that the School and such Data Controllers are all responsible to you for the processing your Personal Data and in the event of any data breaches.

DFE

The School shares Personal Data with the DFE on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to the School funding / expenditure and the assessment educational attainment.

DFE DATA COLLECTION REQUIREMENTS

The following is the information provided by the DFE concerning the reason(s) why it collects data about school employees:

- The DFE collects and processes Personal Data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.
- To find out more about the data collection requirements placed on the School by the DFE including the Personal Data that the School shares with the DFE, please visit: <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.
- The DFE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff by:
 - Conducting research or analysis;
 - Producing statistics; and / or
 - Providing information, advice or guidance.
- The DFE has robust processes in place to ensure that the confidentiality of Personal Data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DFE releases Personal Data to third parties are subject to a strict approval process and based on a detailed assessment of:
 - Who is requesting the Personal Data;
 - The purpose for which the Personal Data is required;
 - The level and sensitivity of Personal Data requested; and
 - The arrangements in place to securely store and handle the Personal Data.

To be granted access to the School workforce information, organisations must comply with the DFE's strict terms and conditions covering the confidentiality and handling of Personal Data, security arrangements and retention and use of Personal Data.

- For more information about the DfE's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>
- To contact the DFE, please visit: <https://www.gov.uk/contact-dfe>

16. THIRD PARTY SERVICE PROVIDERS

HOW SECURE IS YOUR PERSONAL DATA WITH THIRD PARTY SERVICE PROVIDERS

All third-party service providers are required to take appropriate security measures to protect your Personal Data in line with the School's policies. The School does not allow its third-party service providers to use your Personal

Data for their own purposes. The School only permits its third-party service providers to process your Personal Data for specified purposes and in accordance with the School's instructions.

WHAT ABOUT OTHER THIRD PARTIES

The School may share your Personal Data with other third parties, with a regulator or to otherwise comply with the law. From time to time, the School may disclose your Personal Data in response to a request for information pursuant to the Freedom of Information Act 2000 or following a SAR. The School may approach you for your consent but, in any event, the School will only disclose your Personal Data if the School is satisfied that it is reasonable to do so in all the circumstances. Accordingly, the School may refuse to disclose some or all of your Personal Data following receipt of such a request.

Personal Data may be transferred to other countries within the EU borders only (unless there is a legitimate reason to store the Personal Data outside of the EU or your consent has been obtained) if, for example, the School is arranging a school trip to a different country.

17. DATA SECURITY

The School has put in place measures to protect the security of your Personal Data and details of these measures are available upon request. The School has put in place appropriate security measures to prevent your Personal Data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, the School limits access to your Personal Data to those employees, agents, contractors and other third parties who have a business need to know and such persons will only process your Personal Data on the School's instructions and they are subject to a duty of confidentiality.

18. SUSPECTED BREACH OF DATA SECURITY

The School has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where the School is legally required to do so.

19. DATA RETENTION

HOW LONG WILL THE SCHOOL USE YOUR PERSONAL DATA FOR

The School will retain your Personal Data for no longer than what is necessary to fulfil the purposes for which the School collected your Personal Data, including but not limited for the purposes of satisfying any legal, accounting, insurance or reporting requirements. The School's Management and Retention of Records Policy sets out how long the School keeps information about its members of staff. Copies of all policies can be found on the School website.

CONSIDERATIONS FOR DATA RETENTION PERIODS

To determine the appropriate retention period for Personal Data, the School considers the following:

- The amount, nature, and sensitivity of the Personal Data;
- The potential risk of harm from unauthorised use or disclosure of your Personal Data;
- The purposes for which the School process your Personal Data;
- Whether the School can achieve those purposes through other means; and
- The applicable legal requirements.

In some circumstances, the School may anonymise your Personal Data so that it can no longer be associated with you, in which case the School may use such Personal Data without further notice to you. Once you are no longer an employee, worker or contractor of the School the School will retain and securely destroy your Personal Data in accordance with the School's Management and Retention of Records Policy **or** applicable laws and regulations.

20. RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

YOUR DUTY TO INFORM THE SCHOOL OF CHANGES

It is important that the Personal Data we hold about you is accurate and current. Please keep the School informed of your Personal Data changes during your working relationship with the School.

YOUR RIGHTS IN CONNECTION WITH PERSONAL DATA

Under certain circumstances, by law you have the right to:

- **Be informed** as to the collection of your Personal Data, including the reason for the collection of such data, for how long such data will be retained for and with whom such data will be shared with.
- **Request access** to your Personal Data (SAR). This right enables you to receive a copy of the Personal Data the School holds about you and to check that the School is lawfully processing such data for the specified purpose. If requested, Personal Data must be available in a commonly used electronic format.
- **Request rectification** of the Personal Data that the School holds about you. This enables you to have any incomplete or inaccurate Personal Data the School holds about you to be corrected.
- **Request erasure** of your Personal Data. This right enables you to ask the School to delete or remove your Personal Data where it is no longer necessary or relevant for the School to process your Personal Data or where you have withdrawn your consent to the use your Personal Data.
- **Object/restriction to processing** of your Personal Data where the School is relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where (a) the School is processing your Personal Data for direct marketing, research and statistic purposes; (b) you contest the accuracy of the Personal Data; or (c) your Personal Data has been processed unlawfully.
- **Data portability** of your Personal Data. This right enables you to obtain and reuse your Personal Data for your own purposes and have the right to transfer your Personal Data electronically in a safe and secure way.
- **Challenge decisions** made by automated means or profiling.

ENFORCEMENT OF RIGHTS

If you want to review, verify, correct or request erasure of your Personal Data, object to the processing of your Personal Data, or request that the School transfers a copy of your Personal Data to another party, please contact the DPO in writing (details can be found in section 24).

21. SUBJECT ACCESS REQUESTS

Information on SAR, is as follows:

- **Time to respond**: The School will respond to a SAR without undue delay and in any event within one (1) month of receipt of the request. The School may extend the deadline to respond to a SAR by up to two (2) months (so up to three (3) months in total) where the SAR is particularly complex or numerous and if this is the case the School will contact the requestor within one (1) month of making the request and inform he or she why such extension is necessary.
- **Charges**: The school will provide the information requested free of charge.
- **Excessive/unfounded Requests**: The School may charge a reasonable fee if the request for information is manifestly excessive or unfounded, particularly if the request is repetitive. The fee charged will be determined on the basis of the administrative costs of complying with the request and therefore the level of the fee will vary depending on the remit of the request and the administrative costs incurred. The School will need to provide evidence to the requestor on how the request for information is manifestly excessive or unfounded.
- **Unwarranted Requests**: The School may refuse to respond to unwarranted requests for information. The School will explain the reason of refusal to the requestor; inform the requestor of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at least within one (1) month.
- **Electronic requests**: The right to request information may be submitted electronically to the School via the Subject Access Request (SAR) Pro Forma form, unless otherwise requested by the individual. Also, the requestor may make a SAR using any Facebook page or Twitter account that the School has, other social-media sites to which the School subscribes, or via third party websites. The School cannot insist on the use of a particular means of delivery for a SAR.
- **Term time applications for SAR**: As the School has limited staff resources outside of term time, the School encourages the submission of SAR during term time and to avoid sending a request during periods when

the School is closed or is about to close for the holidays where possible. This will assist the School in responding to your request as promptly as possible.

- **Right to Withhold Personal Data:** The School has the right to withhold the disclosure of Personal Data upon a SAR if disclosure would adversely affect the rights and freedoms of others.

For further information about how we handle SAR, please see the School's Data Protection Policy.

22. RIGHT TO WITHDRAW CONSENT

In the limited circumstances, where you may have provided your consent to the collection, processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once the DPO has received notification that you have withdrawn your consent, the School will no longer process your Personal Data for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

23. COMPLAINTS

The School takes any complaints about its collection and use of Personal Data very seriously. If you have a concern about the way the School is collecting or using your Personal Data, you should raise your concern with the School in the first instance. To make a complaint, please contact our DPO. Alternatively, you can make a complaint to the ICO:

- Report a concern online at: <https://ico.org.uk/make-a-complaint/>
- Call: 0303 123 1113 (local rate) or 01625 545 745 (if you prefer to use a national rate number).
- Write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

24. CONTACT US

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

- AGAS Data Protection Officer - Dataprotectionofficer@koinoniafederation.com

25. CHANGES TO THIS PRIVACY NOTICE

The School reserves the right to update this privacy notice at any time, and the School will provide you with a new privacy notice when substantial updates are made. The School may also notify you in other ways from time to time about the processing of your Personal Data.

APPENDIX 3: PRIVACY NOTICE – HOW WE USE PARENT/CARER INFORMATION

1. GENERAL

The School collects a lot of data and information about its pupils so that we can run effectively as a school. This privacy notice explains how and why we collect pupils' and parents and/or carers Personal Data, what we do with such data and what rights parents and/or carers (hereafter referred to as "you" or "your") and pupils (hereafter referred to as "you" or "your") have in relation to the use of such data, that is, in accordance with the GDPR.

2. DEFINITIONS

PARENT

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the pupil, with whom the pupil lives or whether the pupil has contact with that parent), and also includes non-parents who have parental responsibility for the pupil, or with whom the pupil lives. It is therefore possible for a pupil to have several "parents" for the purposes of education law.

OTHER MEMBERS

This privacy notice also covers other members of pupils' families who we may process data about from time to time, including, for example, siblings, aunts and uncles and grandparents.

3. DATA PROTECTION OFFICER ("DPO")

The AGAS Data Protection Officer will:

- Inform and advise the School and its staff members about their obligations to comply with the GDPR and other data protection laws.
- Monitor the School's compliance with the GDPR and other data protection laws, including managing internal data protection activities, conducting internal audits and providing the required training to staff members.
- Report to the highest level of management in the School, which is the Headteacher.

4. DATA PROTECTION LEAD ("DPL")

The DPL for the School is Matthew Wills. The DPL will:

- Ensure the school is in line with GDPR compliance and knows its responsibilities as the Data Controller.
- To liaise with the DPO in accordance to GDPR regulations and Data Breaches.

5. WHY DO WE COLLECT AND USE PARENT/CARER INFORMATION

The School collects and uses parent / carer Personal Data when the law allows the School to do so. Most commonly, the School will use your Personal Data in the following circumstances:

- Where the School has obtained the consent of the Data Subject and this consent can be withdrawn at any time. The School will make this process clear when consent is sought and will explain in detail how consent can be withdrawn.
- Where the School needs to comply with a legal obligation.
- Where processing is necessary to protect the vital interests of the Data Subject or another person.

- Where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

Where the Personal Data the School collect about parents / carers is Special Categories of Personal Data, the School will only process such data where:

- a. The School has explicit consent (unless reliance on consent is prohibited by the EU or Member State law);
- b. The School needs to carry out its legal obligations and in line with its Data Protection Policy;
- c. Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the data subject is physically or legally incapable of giving consent or where the information is already made public;
- d. Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where the School respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject; and/or
- e. The School has obligations or rights under any law.

Please see the School Data Protection Policy for a definition of Special Categories of Personal Data.

6. SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL DATA

The situations in which the School will process Personal Data about the parents / carers are listed below:

- To decide who to admit to the School.
- To maintain a waiting list.
- To support pupil learning.
- To monitor and report on pupil progress.
- To provide appropriate pastoral care.
- To assess the quality of the School services.
- To comply with the law regarding data sharing.
- For the protection and welfare of pupils and others in the School, including our safeguarding / child protection obligations.
- For the safe and orderly running of the School.
- To promote the School.
- To send parent / carer communications that may be of interest, which may include information about School events or activities, news, campaigns, appeals and other fundraising activities.
- In order to respond to investigations from the School's regulators or to respond to complaints raised by the School stakeholders.
- In connection with any legal proceedings threatened or commenced against the School.

This list is not exhaustive

7. CATEGORIES OF PERSONAL DATA HELD BY THE SCHOOL ABOUT THE PARENT / CARER

The School may collect, store, use and share (where appropriate) the following categories of Personal Data about parents / carers:

- Personal information (such as name, address, telephone number and email address).
- Information relating to your identity.
- Marital status.
- Employment status.
- Religion.
- Ethnicity.
- Language.
- Medical conditions.
- Nationality.
- Country of birth.

- Free school meal / pupil premium eligibility / entitlement to certain benefits.
- Information about court orders in place affecting parenting arrangements for pupils).

From time to time and in certain circumstances, the School might also process personal data about parents / carers, some of which might be sensitive personal data, as follows:

- Information about criminal proceedings / convictions; or
- Information about child protection / safeguarding.

This information is not routinely collected about parents / carers and is only likely to be processed by the school in specific circumstances relating to particular pupils, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police.

Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure. The School collects information about parents / carers before pupils join the School and update it during pupils' time on the roll as and when new information is acquired.

COLLECTING PARENT / CARER INFORMATION

Whilst the majority of information about parents / carers provided to the School is mandatory, some of it is provided to the School on a voluntary basis. In order to comply with the GDPR, the School will inform you whether you are required to provide certain parent / carer information to the School or if you have a choice in this. Where appropriate, the School will ask parents / carers for consent to process Personal Data where there is no other lawful basis for processing it, for example where the School wishes to ask your permission to use your information for marketing purposes or to request voluntary contributions. Parents / carers may withdraw consent given in these circumstances at any time.

In addition, the School also uses CCTV cameras around the School site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or to investigate other issues. CCTV footage involving parents / carers will only be processed to the extent that it is lawful to do so. Please see the School's Management and Retention of Records Policy for more details.

8. STORING PERSONAL DATA

The School keeps Personal Data about parents / carers in order to comply with its legal obligations. A significant amount of Personal Data is stored electronically, for example, on the School database. Some Personal Data may also be stored in hard copy format. Personal Data stored electronically may be saved on a cloud-based system which may be hosted in a different country, that is, within the EU border only (unless there is a legitimate reason to store the Personal Data outside of the EU or consent of the Data Subject has been obtained).

Personal Data may be transferred to other countries within the EU borders only (unless there is a legitimate reason to store the Personal Data outside of the EU or consent of the Data Subject has been obtained) if, for example, the School is arranging a school trip to a different country. Appropriate steps would be taken to keep the Personal Data secure. The School's Management and Retention of Records Policy sets out how long the School keeps information about its pupils and parents / carers. Copies of all policies can be found on the School website.

To determine the appropriate retention period for Personal Data, the School will consider the following:

- The amount, nature, and sensitivity of the Personal Data.
- The potential risk of harm from unauthorised use or disclosure of your Personal Data.
- The purposes for which the School process your Personal Data.
- Whether the School can achieve those purposes through other means.

- The applicable legal requirements

In some circumstances, the School may anonymise your Personal Data so that it can no longer be associated with you, in which case the School may use such information without further notice to you. Once you are no longer a parent / carer of a child at the School, the School will retain and securely destroy your Personal Data in accordance with the School's Management and Retention of Records Policy or applicable laws and regulations.

9. DATA SHARING

WHO DOES THE SCHOOL SHARE PARENT / CARER PERSONAL DATA WITH?

The School does not share Personal Data about parent / carers without their consent (unless the law or the School policies allow the School to do so). The School may share parent / carer Personal Data with:

- Schools that pupils attend after leaving the School.
- Greenwich Safeguarding Board.
- Special Educational Needs and Disability
- The local authority, that is, Greenwich to meet legal obligations to share certain information with it.
- A pupil's home local authority (if different).
- The Department for Education (DFE) (on a statutory basis) to find out more about the data collection requirements placed on the School by the DFE (for example the School census) go to: <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.
- The School local governors.
- The Police and law enforcement agencies.
- The NHS health professionals including the School nurse and educational psychologists.
- Education Welfare Officers.
- Courts and tribunals (if ordered to do so).
- The Teaching Regulation Agency.
- The prevent teams in accordance with the Prevent Duty on schools.
- Other schools, for example, if the School is negotiating a managed move and the School has obtained your consent to share information in these circumstances.
- Diocesan Officers at the Southwark Diocesan Board of Education for the purposes of receiving educational support.
- The School's legal advisors.
- Insurance providers / the Risk Protection Arrangement.

This list is not an exhaustive list

Some of the organisations referred to above are joint Data Controllers. This means that all of the above (including the School) are all responsible to you for how we process your Personal Data. In the event that the School shares Personal Data about parents / carers with third parties, the School will provide the minimum amount of Personal data necessary to fulfil the purpose for which we are required to share the data.

10. SUBJECT ACCESS REQUESTS ("SAR")

Under the GDPR, parents / carers have the right to request access to information about them that the School holds.

To make a request for your Personal Data, please contact the School's Data Protection Lead although any written request for Personal Data will be treated as a SAR.

Information on SAR, is as follows:

- **Information required:** The School may need to request specific information from you to help the School confirm your identity and ensure your right to access the information (or to exercise any of your rights). This is another appropriate security measure to ensure that your Personal Data is not disclosed to any person who has no right to receive it. You also have the right to:
 - Object to processing of Personal Data that is likely to cause, or is causing, damage or distress.
 - Prevent processing for the purpose of direct marketing.

- Object to decisions being taken by automated means;
- In certain circumstances, have inaccurate Personal Data rectified, blocked, erased or destroyed.
- Claim compensation for damages caused by a breach of the School's data protection responsibilities.
- **Time to respond:** The School will respond to a SAR without undue delay and in any event within one (1) month of receipt of the request. The School may extend the deadline to respond to a SAR by up to two (2) months (so up to three (3) months in total) where the SAR is particularly complex or numerous and if this is the case the School will contact the requestor within one (1) month of making the request and inform he or she why such extension is necessary.
- **Charges:** The school will provide the information requested free of charge.
- **Excessive/unfounded Requests:** The School may charge a reasonable fee if the request for information is manifestly excessive or unfounded, particularly if the request is repetitive. The fee charged will be determined on the basis of the administrative costs of complying with the request and therefore the level of the fee will vary depending on the remit of the request and the administrative costs incurred. The School will need to provide evidence to the requestor on how the request for information is manifestly excessive or unfounded.
- **Unwarranted Requests:** The School may refuse to respond to unwarranted requests for information. The School will explain the reason of refusal to the requestor, inform the requestor of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at least within a month.
- **Electronic requests:** The right to request information may be submitted electronically to the School using the SAR Pro Forma form, unless otherwise requested by the individual. Also, the requestor may make a SAR using any Facebook page or Twitter account that the School has, other social-media sites to which the School subscribes, or via third party websites. The School cannot insist on the use of a particular means of delivery for a SAR.
- **Term time applications for SAR:** As the School has limited staff resources outside of term time, the School encourage the submission of SAR during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist the School in responding to your request as promptly as possible.
- **Right to Withhold Personal Data:** The School has the right to withhold the disclosure of Personal Data upon a SAR if disclosure would adversely affect the rights and freedoms of others.

For further information about how we handle Subject Access Requests, please see the School's Data Protection Policy.

11. RIGHT TO WITHDRAW CONSENT

In the limited circumstances, where you may have provided your consent to the collection, processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once the DPO has received notification that you have withdrawn your consent, the School will no longer process your Personal Data for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

12. COMPLAINTS

The School takes any complaints about its collection and use of Personal Data very seriously. If you have a concern about the way the School is collecting or using your Personal Data, you should raise your complaint with the School in the first instance. To make a complaint, please contact our DPO. Alternatively, you can make a complaint to the ICO:

- Report a concern online at: <https://ico.org.uk/make-a-complaint/>
- Call: 0303 123 1113 (local rate) or 01625 545 745 (if you prefer to use a national rate number)

Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

13. CONTACT US

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

- AGAS Data Protection Officer –Dataprotectionofficer@koinoniafederation.com

13. CHANGES TO THIS PRIVACY NOTICE

The School reserves the right to update this privacy notice at any time, and the School will provide you with a new privacy notice when substantial updates are made.

The School may also notify you in other ways from time to time about the processing of your Personal Data.