

Haggerston School

Data Protection Policy

Author	School Business Leader
Date Completed	24 th September 2018
Date to be Reviewed	September 2019
Version	01/2018

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions.....	3
4. The data controller	4
5. Roles and responsibilities	4
6. Data protection principles.....	4
7. Collecting personal data.....	5
8. Sharing personal data	5
9. Subject access requests and other rights of individuals	6
10. Parental requests to see the educational record	7
11. Biometric recognition systems.....	7
12. CCTV	7
13. Photographs and videos	7
14. Data protection by design and default	8
15. Data security and storage of records.....	8
16. Disposal of records	9
17. Personal data breaches	9
18. Training.....	9
19. Monitoring arrangements	9
Appendix 1: Personal data breach procedure	10
Appendix 2: The General Data Protection Regulation (GDPR).....	11
Appendix 3: Privacy Notice - How we use pupil and parent information	12
Appendix 4: Privacy Notice - How we use Staff Information	17
Appendix 5: Privacy Notice - How we use Governors' Information	21
Appendix 6: Privacy Notice - How we use Applicants Information	24
Appendix 7: Privacy Notice - How we use Trainee Information	26
Appendix 8: Privacy Notice - How we use Supply Staff, Consultants and Contractors' Information.....	29

1. Aims

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

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

2. Legislation and guidance

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

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

3. Definitions

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

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

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

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing Body

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

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

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

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

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

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for schools](#).

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

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

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

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

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

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

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

9.3 Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

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

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

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

10. Parental requests to see the educational record

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

11. Biometric recognition systems

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

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

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

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

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the Premises Manager (premises@sjcr.net).

13. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding policy for more information on our use of photographs and videos.

14. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

18. Training

All staff and governors will be provided with data protection training.

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

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

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the internal school breach register, and in the school electronic and paper filing systems. Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the internal school breach register, and in the school electronic and paper filing systems. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Appendix 2: The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which will determine how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

Types of data

- 'Personal data' means information that can identify a living individual.
- 'Sensitive personal data' means personal data consisting of information as to ethnicity, religion, sexuality, political views, etc).

The regulation will apply to all schools from the **25th May 2018** and will apply even after the UK leaves the EU.

Main principles

The GDPR sets out the **key principles** that all personal data must be processed in line with.

- Data must be: processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

There are also **stronger rights for individuals** regarding their own data.

- **The individual's rights include:** to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

New requirements

The GDPR is similar to the Data Protection Act (DPA) 1998 (which schools already comply with), but strengthens many of the DPA's principles. The main changes are:

- Schools must appoint a data protection officer, who will advise on compliance with the GDPR and other relevant data protection law.
- Privacy notices must be in clear and plain language and include some extra information – the school's 'legal basis' for processing, the individual's rights in relation to their own data.
- Schools will only have a month to comply with subject access requests, and in most cases can't charge.
- Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous.
- There are new, special protections for children's data.
- The Information Commissioner's Office must be notified within 72 hours of a data breach.
- Organisations will have to demonstrate how they comply with the new law.
- Schools will need to carry out a data protection impact assessment when considering using data. in new ways, or implementing new technology to monitor pupils.
- Higher fines for data breaches – up to 20 million euros or 4% of global annual turnover.

Conditions for processing data

Conditions for Processing Personal data (Name, address, DoB etc)	Conditions for processing 'Special' categories data (SEN, family, bank, salary, sexuality, criminal records)
Consent	Explicit consent
Necessary for contract	Necessary for field of employment and social security
Necessary for legal obligation	Vital interests where person physically or legally incapable of not giving consent
Vital Interests (in the absence of other conditions)	Manifestly made public by data subject
Necessary for official authority/task carried out in the public interest – (Schools)	Necessary for establishment
Necessary for legitimate interest	

Appendix 3: Privacy Notice - How we use pupil and parent information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you and your child(ren) at our school, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If any information linked to you is unclear, please contact the School Registrars or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, Haggerston School at Weymouth Terrace, London E2 8LS are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO). The contact details are: Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

1. The categories of pupil & parent information that we collect, hold and share include but are not limited to:

- Personal information (such as name, unique pupil number and address, parents' national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as data scores, tracking, and internal and external testing)
- Relevant medical information (such as NHS information, health checks, physical and mental health care, immunisation program and allergies)
- Special educational needs information (such as EHCP's, statements, applications for support, care or support plans)
- Safeguarding information
- Exclusion information
- Behavioural information
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- CCTV images
- Payment details for Bursaries
- Biometric data for school meals
- Genetic data

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

2. Why we collect and use this information

We use the pupil and parent data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral and medical care
- for safeguarding and pupil welfare purposes
- administer admissions waiting lists
- for research purposes
- to inform you about events and other things happening in the school
- to assess the quality of our services
- to comply with the law regarding data sharing

3. The lawful basis on which we use this information

Our lawful basis for collecting and processing pupil information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- (a) Data subject gives consent for one or more specific purposes.
- (c) Processing is necessary to comply with the legal obligations of the controller.
- (d) Processing is necessary to protect the vital interests of the data subject.
- (e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing pupil information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
- (b) It is necessary to fulfill the obligations of controller or of data subject.
- (c) It is necessary to protect the vital interests of the data subject.
- (d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- (g) Reasons of public interest in the area of public health
- (i) It is in the public interest

A full breakdown of the information we collect on pupils can be requested by the School's Student & Data Services.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

An example of how we use the information you provide is:

The submission of the school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996.

Putting the school census on a statutory basis:

- means that schools do not need to obtain parental or pupil consent to the provision of information
- ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils
- helps to ensure that returns are completed by schools

4. Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

5. Storing pupil data

We hold pupil data whilst the child remains at Haggerston School. The file will follow the pupil when they leave Haggerston School and will be retained based on the Date of Birth of the pupil + 25 years. However where there is a legal obligation to retain the information beyond that period, it will be retained in line with our retention policy.

Please refer to the School's Data Storage and Retention Policy (Information Management Toolkit for Schools) for further information:

<https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22>

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

6. **Who we share pupil information with**

We routinely share pupil information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- schools that the pupil's attend after leaving us

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

7. **Why we share pupil information**

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

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

8. **Data collection requirements:**

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

9. **Youth support services**

Pupils aged 13+ [For use by educational settings with students aged 13+:]

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

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16+ [For use by educational settings with students aged 16+:]

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

This enables them to provide services as follows:

- post-16 education and training providers

- youth support services
- careers advisers

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

10. The 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.

We are required by law, to provide information about our 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 NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with 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

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether 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 it is required
- the level and sensitivity of data requested: and
- 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 DfE: <https://www.gov.uk/contact-dfe>

11. Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold, through a Subject Access Request.

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

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

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

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

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

If you would like to make a request please contact our data protection officer.

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

Parents/carers also have a legal right to access to their child's educational record. To request access, please contact the School's Student & Data Services.

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; and
- claim compensation for damages caused by a breach of the Data Protection regulations

12. Complaints

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

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

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161

e-mail: Robert.Bullett@london.anglican.org

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

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

13. Contact us

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

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

or

Student & Data Services: student.dataservices@haggerston.hackney.sch.uk

Data Manager: 020 7739 7324 ext. 4587 / Admissions Officer: 020 7739 7324 ext. 4544

Appendix 4: Privacy Notice - How we use Staff Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as our employees at our school, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If any information linked to you is unclear, please contact the HR Manager or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, Haggerston School at Weymouth Terrace, London E2 8LS are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO). The contact details are: Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

1. The categories of staff information that we collect, hold and share include but are not limited to:

- Personal information (such as name, address, national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth)
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your entitlement to work in the UK
- information about your criminal record
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments and fulfil its duty of care (including the use of Occupational Health Services)
- details of trade union membership where provided by yourself or your trade union
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief (where this has been provided)
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes)
- CCTV images

We may also hold personal data about you from third parties, such as references supplied by former employers, information provided during the completion of our pre-employment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

2. Why we collect and use this information

The purpose of collecting and processing this data is to help us recruit staff and run the school efficiently, including to:

- Enable you to be paid and other benefits be provided
- Facilitate our safer recruitment of staff, as part of our safeguarding obligations towards pupils
- Fulfil our legal obligations in recruiting staff
- Support effective performance management and appraisal
- Support effective management of the school workforce, along with the implementation of its policies and procedures
- Inform our recruitment and retention policies

- Allow better financial modelling, administration and planning
- Provide references where requested
- Equalities monitoring and reporting
- Respond to any staffing issues
- Improve the management of workforce data across the sector
- to assess the quality of our services
- to comply with the law regarding data sharing

3. The lawful basis on which we use this information

Our lawful basis for collecting and processing staff information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- (a) Data subject gives consent for one or more specific purposes.
- (c) Processing is necessary to comply with the legal obligations of the controller.
- (d) Processing is necessary to protect the vital interests of the data subject.
- (e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
- (b) It is necessary to fulfill the obligations of controller or of data subject.
- (c) It is necessary to protect the vital interests of the data subject.
- (d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- (h) Processing 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
- (i) It is in the public interest.

A full breakdown of the information we collect on staff can be requested from the HR Manager.

Where we have obtained consent to use staff members personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

4. Collecting staff information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

5. Storing your data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our retention policy.

Please refer to the School's Data Storage and Retention Policy (Information Management Toolkit for Schools) for further information: <https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22>

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

6. Who we share information with

We routinely share staff information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information relating to certain staffing matters
- The Department for Education - to meet our legal obligations to share certain information with it,
- Your family and representatives – such as in the event of an emergency

- Educators and examining bodies – such as ensuring we adhere to examining regulations to guarantee the validity of examinations
- Ofsted – such as during the course of a school inspection
- Suppliers and service providers – to enable them to provide the service we have contracted them for e.g. HR, payroll, employee benefit schemes
- Financial organisations e.g. Pension Scheme
- Central and local government – such as workforce analysis
- Our auditors, to ensure our compliance with our legal obligations
- Trade Unions and Professional Associations - to enable them to provide the service their members require
- Health authorities and Occupational Health and employee support schemes – to ensure the wellbeing of our staff body in accordance with our responsibilities as employer
- Security organisations – to create a secure workplace for staff
- Health and social welfare organisations – to ensure the wellbeing of our staff body in accordance with our responsibilities as employer
- Professional advisers and consultants – for us to develop our service to best provide our public service
- Charities and voluntary organisations -
- Police forces, courts, tribunals
- Employment and recruitment agencies
- Future employers

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

7. Why we share your information

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

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment. We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

8. Data collection requirements:

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

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

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

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

- who is requesting the data

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

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

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>

To contact the department: <https://www.gov.uk/contact-dfe>

9. Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, staff members have the right to request access to information about them that we hold, through a Subject Access Request.

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

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

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

If you would like to make a request please contact our data protection officer.

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

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; and
- claim compensation for damages caused by a breach of the Data Protection regulations

10. Complaints

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

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

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

If you would like to make a request please contact our data protection officer.

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

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

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

11. Contact us

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

or **HR Manager**: email: hr.dept@haggerston.hackney.sch.uk

Appendix 5: Privacy Notice - How we use Governors' Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as governors at our school, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If any information linked to you is unclear, please contact the HR Manager or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, Haggerston School at Weymouth Terrace, London E2 8LS are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO). The contact details are: Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

1. The categories of information that we collect, hold and share include but are not limited to:

- Personal information (such as name, address,).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- details of your qualifications, skills, and experience for skills audit purposes;
- information about your criminal record;
- details of your appointment, including the appointing body, the date of appointment, and term of office.
- Training you have attended in your role as a governor
- Your attendance and visits to the school in your role as a governor
- Any roles or leadership responsibilities you hold within the governing body
- Your business or other charitable interests
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief (where this has been provided)
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes)
- CCTV images

We may also hold personal data about you from third parties, such as information supplied by the appointing body and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

2. Why we collect and use this information

The purpose of collecting and processing this data is to:

- Enable you to serve as a governor
- Comply with our statutory safeguarding obligations
- Ensure we comply with our instrument of governance / Articles of Association
- Support effective governor development
- Support effective management of the school
- Statutory reporting to the Department for Education
- Equalities monitoring and reporting
- Respond to any governance issues
- Improve the management of workforce data across the sector
- to assess the quality of our services
- to comply with the law regarding data sharing

3. The lawful basis on which we use this information

Our lawful basis for collecting and processing your information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- (c) Processing is necessary to comply with the legal obligations of the controller.
- (e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
- (b) It is necessary to fulfill the obligations of controller or of data subject.
- (d) Processing is carried out by a foundation or not-for-profit organization (includes religious, political or philosophical organizations and trade unions)
- (i) It is in the public interest.

A full breakdown of the information we collect on governors can be requested from the HR Manager.

Where we have obtained consent to use governors members personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

4. Collecting Governor information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

5. Storing your data

We create and maintain a file for each governing body member. The information contained in this file is kept secure and is only used for purposes directly relevant to your term as a governor at the school. Once your term(s) of office with us has ended, we will retain this file and delete the information in it in accordance with our retention policy.

Please refer to the School's Data Storage and Retention Policy (Information Management Toolkit for Schools) for further information:

<https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22>

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

6. Who we share information with

We routinely share information with appropriate third parties, including:

- The Department for Education - to meet our legal obligations to share certain information with it
- Ofsted
- Our auditors, to ensure our compliance with our legal obligations
- Professional advisers and consultants – for us to develop our service to best provide our public service
- Police forces, courts, tribunals

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

7. Why we share your information

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

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. Under s.538 of the Education Act 1996, and the Academies Financial Handbook, the Secretary of State requires boards to provide certain details they hold about people involved in governance, as volunteered by individuals, and the information kept up to date.

8. Data collection requirements:

The DfE collects and processes personal data relating to those governing schools (including Single and Multi Academy Trusts and all schools are required to ensure they keep their governors details up to date under s.538 of the Education Act 1996, and the Academies Financial Handbook

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

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

To contact the department: <https://www.gov.uk/contact-dfe>

9. Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, governors have the right to request access to information about them that we hold, through a Subject Access Request.

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

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

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

If you would like to make a request please contact our data protection officer.

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161

e-mail: Robert.Bullett@london.anglican.org

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; and
- claim compensation for damages caused by a breach of the Data Protection regulations

10. Complaints

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

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

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161

e-mail: Robert.Bullett@london.anglican.org

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

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

11. Contact us

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

or **HR Manager**: email: hr.dept@haggerston.hackney.sch.uk

Appendix 6: Privacy Notice - How we use Applicants Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as applicants at our school, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If any information linked to you is unclear, please contact the HR Manager or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, Haggerston School at Weymouth Terrace, London E2 8LS are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO). The contact details are: Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

We collect all the information laid out in this form, in the form of references from current and/or previous employers, and if shortlisted from the selection process. The information given to us, and collected by us will form part of the contract of employment for successful candidates. We process this information in order to:

- administer the application, shortlisting and selection process
- assess your suitability to work with children and young people
- inform the development of recruitment and retention policies
- defend legal claims
- fraud detection and prevention
- monitor protected characteristics in order to promote equality at work

No decisions are based on automated decision making.

We process this information about you because the processing is necessary for us to enter into an employment (or other work-related) contract with you. We also need to process this information to ensure that we are complying with our legal obligations under the Employment Act and with the DfE statutory guidance document, Keeping Children Safe in Education, as well as other school specific legislation.

We have a legitimate interest in processing data from job applicants in order to administer the recruitment process, to monitor compliance with our policies, to defend any legal claims and to ensure that the most suitable applicant is appointed to the role, based on an assessment of their likely performance amongst other factors.

We process special category data, such as information about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations. This information is collected with the express consent of job applicants. Consent may be withdrawn by an applicant at any time.

We may offer to contact unsuccessful applicants within a period of six months following the application if another suitable vacancy arises. Information is only used in this way with the express consent of applicants, which may be withdrawn at any time.

If we wish to process your personal data for a new purpose we will inform you of any additional processing.

Information from your application form and from the shortlisting and selection process will be stored in a paper-based file, in electronic records within our HR system and also in other IT systems, including email.

A copy of your application form and all other personal data collected during the recruitment and selection process will be held as follows:

- For successful applicants this will be transferred to a personnel file where it will be held securely. You will be given a workforce privacy notice upon appointment which will explain how we will hold and process your data as an employee.
- For unsuccessful applicants, securely for a period of six months minimum.

Your information will be shared with school staff with a recruitment responsibility. This will include members of our HR and administrative staff, those responsible for shortlisting and interviewing and managers within the relevant area of work or department. Equality monitoring information is separated from the application form upon receipt and is not shared with those responsible for shortlisting and interviewing.

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

We will not share your data with third parties unless and until an offer of employment is made to you. At that stage, your data will be shared to fulfil legal requirements, obtain or provide necessary information or because the third party processes data on our behalf. These third parties include:

- The Disclosure and Barring Service in order to undertake a criminal record check
- Suppliers and consultants that provide us with a service, such as occupational health, HR or legal services
- Relevant professional bodies in order to verify your qualifications (such as the Teaching Regulation Agency for teaching posts).

When we appoint third parties to process data on our behalf, the third party is also required to process the data lawfully and fairly and in a manner that ensures appropriate security of the data, using appropriate technical or organisational measures to protect against unauthorised or unlawful processing and accidental loss.

We do not transfer your data to countries outside the European Economic Area.

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our data protection officer (details at the beginning of this document).

You also have the right to:

- restrict processing of your data in certain circumstances;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- object to the processing of your data where we are relying on our legitimate interests as the lawful basis for processing;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of data protection legislation.

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

If you would like to discuss anything above, please contact the HR Manager:
hr.dept@haggerston.hackney.sch.uk

Appendix 7: Privacy Notice - How we use Trainee Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as a trainee in our school, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If any information linked to you is unclear, please contact the HR Manager or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, Haggerston School at Waymouth Terrace, London E2 8LS are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO). The contact details are: Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

1. The categories of information that we collect, hold and share include but are not limited to:

- Personal information (such as name, address, national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth)
- the terms and conditions of your employment if a paid trainee, including information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your entitlement to work in the UK (where applicable);
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at school;
- details of periods of leave or absence taken by you
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments and fulfil its duty of care (including the use of Occupational Health Services);
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- CCTV images

We may also hold personal data about you from third parties, such as references supplied by former employers, information provided during the completion of our pre-employment checks (where applicable), your application to your training centre, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

2. Why we collect and use this information

The purpose of collecting and processing this data is to help us recruit trainees and run the school efficiently, including to:

- Enable you to be paid and other benefits be provided (where applicable)
- Fulfil our legal obligations towards safeguarding pupils
- Support effective performance management and appraisal and development of trainees
- Provide feedback to your training centre and awarding body
- Provide references where requested
- Equalities monitoring and reporting
- to assess the quality of our services
- to comply with the law regarding data sharing

3. The lawful basis on which we use this information

Our lawful basis for collecting and processing trainee information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- (a) Data subject gives consent for one or more specific purposes.

- (c) Processing is necessary to comply with the legal obligations of the controller.
- (e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
- (b) It is necessary to fulfill the obligations of controller or of data subject.
- (c) It is necessary to protect the vital interests of the data subject.
- (d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)

A full breakdown of the information we collect on staff can be requested from the HR Manager.

Where we have obtained consent to use trainee members personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

4. Collecting trainee information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

5. Storing your data

We create and maintain a file for each trainee. The information contained in this file is kept secure and is only used for purposes directly relevant to your placement with us.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our retention policy.

Please refer to the School's Data Storage and Retention Policy (Information Management Toolkit for Schools) for further information:

<https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22>

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

6. Who we share information with

We routinely share trainees' information with appropriate third parties, including:

- Your training centre
- Your awarding body
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information relating to certain other matters
- The Department for Education
- Educators and examining bodies
- Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Central and local government
- Professional advisers and consultants – for us to develop our service to best provide our public service
- Police forces, courts, tribunals
- Employment and recruitment agencies
- Future employers

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

7. Why we share your information

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

We share information with your training provider in order to provide you with the best possible support.

8. Data collection requirements:

Our data collection requirements relate to our contractual obligations with the training centres with which we work. Further details are available on request.

9. Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, you have the right to request access to information about them that we hold, through a Subject Access Request.

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

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

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

If you would like to make a request please contact our data protection officer.

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

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; and
- claim compensation for damages caused by a breach of the Data Protection regulations

10. Complaints

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

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

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

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

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

11. Contact us

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

or **HR Manager**: email: hr.dept@haggerston.hackney.sch.uk

Appendix 8: Privacy Notice - How we use Supply Staff, Consultants and Contractors' Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as Supply Staff, Consultants and Contractors at our school, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If any information linked to you is unclear, please contact the HR Manager or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, Haggerston School at Weymouth Terrace, London E2 8LS are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO). The contact details are: Robert Bullett at the London Diocesan Board for Schools (Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org)

1. The categories of information that we collect, hold and share include but are not limited to:

- Personal information (such as name, address, national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth)
- the terms and conditions of your deployment with us including contractual terms;
- details of your qualifications, skills, experience and employment history where required;
- Payment details where applicable;
- information about your emergency contacts or associated procedure;
- information about your entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments and fulfil its duty of care (including the use of Occupational Health Services);
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- CCTV images

We may also hold personal data about you from third parties, such as references supplied by former employers or service users, information provided during the completion of our pre-deployment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

2. Why we collect and use this information

The purpose of collecting and processing this data is to help us run the school efficiently, including to:

- Fulfil our legal obligations in relation to Keeping Children Safe in Education
- Develop all aspects of the school operationally
- Inform our operational procedures
- Allow better financial modelling, administration and planning
- Provide references where requested
- Allow us to fulfil or legal and contractual obligations
- to assess the quality of our services
- to comply with the law regarding data sharing

3. The lawful basis on which we use this information

Our lawful basis for collecting and processing your information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- (a) Data subject gives consent for one or more specific purposes.
- (c) Processing is necessary to comply with the legal obligations of the controller.

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
- (b) It is necessary to fulfill the obligations of controller or of data subject.
- (d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)

A full breakdown of the information we collect on Supply Staff, Contractors and Consultants can be requested from the HR Manager.

Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

4. Collecting Your Information

Whilst the majority of information you provide to us is mandatory our related to our mutual contractual obligation, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

5. Storing your data

We create and maintain filing system related to these individuals. The information contained in these files is kept secure and is only used for purposes directly relevant to your deployment with us. Once your deployment with us has ended, we will retain this file and delete the information in it in accordance with our retention policy.

Please refer to the School's Data Storage and Retention Policy (Information Management Toolkit for Schools) for further information:

<https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22>

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

6. Who we share information with

We routinely share supply, contractor and consultant information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Your agency or employer regarding the service provided
- Suppliers and service providers – to enable them to provide the service we have contracted them
- Our auditors, to ensure our compliance with our legal obligations
- Security organisations – to create a secure school environment
- Professional advisers and consultants – for us to develop our service to best provide our public service
- Police forces, courts, tribunals
- Future employers – references

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

7. Why we share your information

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

We only share your information with our Local Authority if we there is a genuine safeguarding concern. The majority of the information shared will be to manage the mutual contractual obligations in place around the services provided.

8. Data collection requirements:

Our data collection requirements all relate to the our legal and contractual obligations, for example contract clauses or the statutory 'Keeping Children Safe in Education Guidance'

9. Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, you have the right to request access to information about you that we hold, through a Subject Access Request.

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

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

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

If you would like to make a request please contact our data protection officer.

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161

e-mail: Robert.Bullett@london.anglican.org

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; and
- claim compensation for damages caused by a breach of the Data Protection regulations

10. Complaints

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

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

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161

e-mail: Robert.Bullett@london.anglican.org

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

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

11. Contact us

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

Name: Robert Bullett

Address: London Diocesan House, 36 Causton Street, London, SW1P 4AU

Tel: 020 7932 1161 / e-mail: Robert.Bullett@london.anglican.org

or **HR Manager**: email: hr.dept@haggerston.hackney.sch.uk