Data Protection policy

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013/2	
Last updated	10.11.2020	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, students, parents, trustees, 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 (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.
In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

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

4. The data controller

Our school processes personal data relating to parents, students, staff, trustees, 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 Trust Board

The Trust 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 Trust 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 **David Coy** and is contactable via **david.coy@london.anglican.org** .

5.3 Head Teacher

The Head Teacher 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 student) 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 students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student 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 student 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 students – 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 students 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 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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 student 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

Academies are not required to provide educational records if a parent requests it, as the Education (student information) Regulations 2005, which places this obligation on maintained schools, does not apply to academies. An academy may choose to comply but parents no longer have a legal right to this information. However, please refer to the section on subject access above.

The Independent School Standards Regulations which applies to academies by virtue of their funding agreement, states that the standard about provision of information is met if the Academy Trust ensures that an annual written report of each registered student's progress and attainment in the main subject areas taught, is sent to the parents of that registered student.

10.1 Fee

Students can request access to their educational record. The cost depends on the number of pages provided. The maximum cost is £50. We charge parents/carers what it costs to supply a copy of the information. It is free for a parent/carer to view their child's educational record in school. https://ico.org.uk/for-the-public/schools/students-info/

11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.[1]

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 students 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 students. For example, students can pay for school dinners using a pin number.

Parents/carers and students 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 student 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 student'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 also have a CCTV Policy, see appendix 10.

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.

[1] In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Any enquiries about the CCTV system should be directed to **Andy Pelton, Facilities Manager**.

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 students aged 18 and over, for photographs and videos to be taken of students 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 student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.
Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. See our child protection and safeguarding policy for more information on our use of photographs and videos.

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 students are reminded to change their passwords at regular intervals
- Personal data must not be extracted from the MIS and then stored on your laptop
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online safety policy/ICT policy/acceptable use agreement)
- 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.

The Richmond upon Thames School records will be kept in line with our student privacy notice.

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 students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

18. Training

All staff and trustees are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. 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**[2] and shared with the full Trust Board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online safety
- Acceptable use agreement
- Child protection and safeguarding policy

[2] The 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 are still new and schools are working out how best to implement them, we will review the data protection policy annually, and then extend this to every 2 years once we are confident with our arrangements.

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 Head Teacher and the chair of trustees
- 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 school's computer system.
- 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 school's computer system

- The DPO and Head Teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

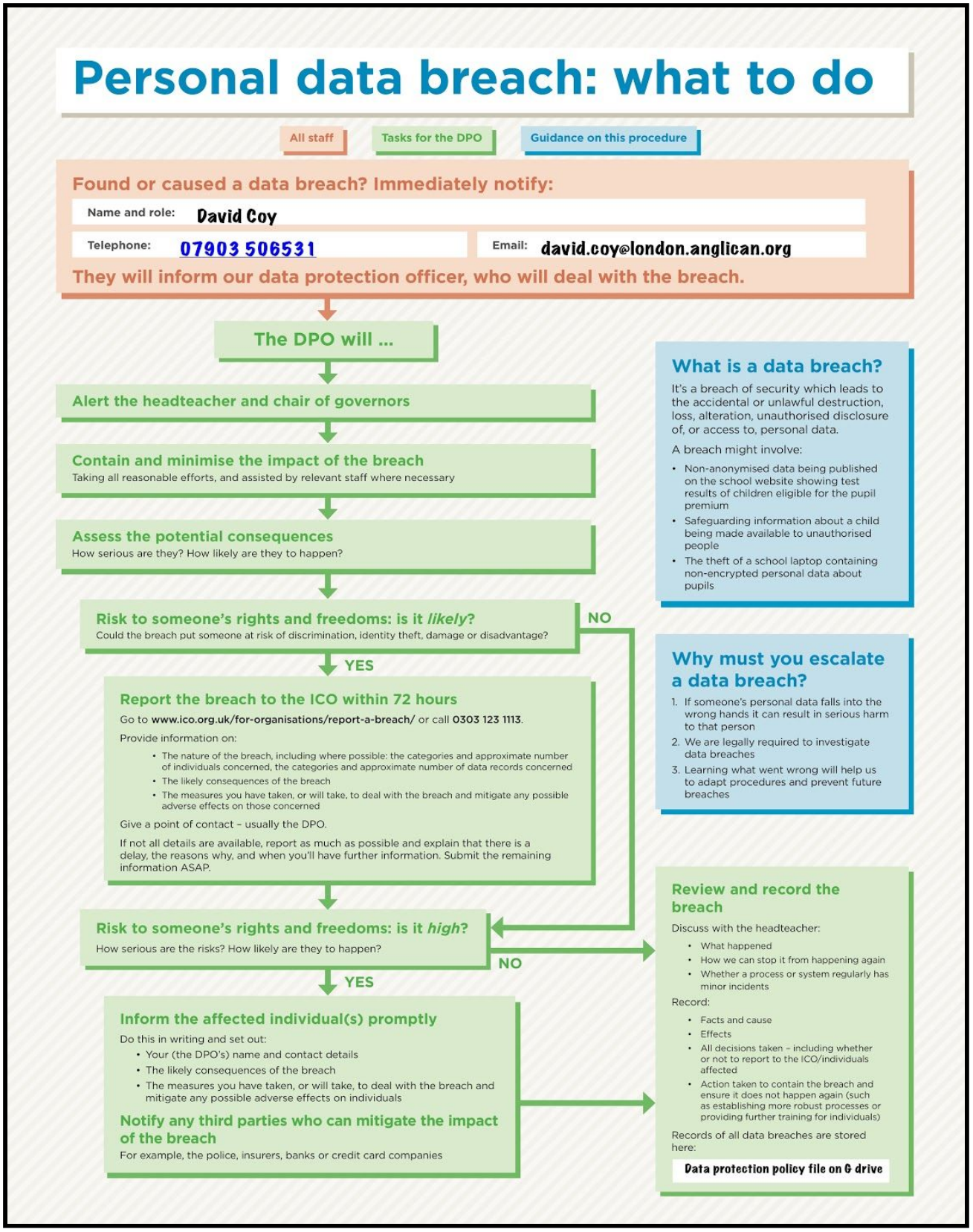
Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

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

- *Details of student premium interventions for named children being published on the school website*
- *Non-anonymised student exam results or staff pay information being shared with trustees*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

Appendix 2 - Data Breach Procedures for staff



Appendix 3 - Record of Data Breaches

Accessible in school.

Appendix 4 - Student Privacy Notice

Student Privacy Notice

How we use student information

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 (Appendix 4)	
Version	Last updated: 03.03.2019	

Introduction

This notice is to help students understand how and why we collect your personal information and what we do with that information. It also explains the decisions that you can make about your own information. We are giving you this notice because you are mature enough to make decisions about your personal information.

If you have any questions about this notice, please talk to your parent/carer.

What is "personal information"?

Personal information is information that the School holds about you. This includes information such as your name, date of birth and address as well as things like exam results, medical details and behaviour records. The School may also record your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

How and why does the School collect personal information?

Admissions forms give us lots of personal information. We get information from you, your teachers and other students. Your old school also gives us information about you so that we can teach and care for you. Sometimes we get information from your doctors and other professionals where we need this to look after you. We collect this information to help the School run properly, safely and to let others know what we do here. Here are some examples:

- We need to tell all your teachers if you are allergic to something or might need extra help with some tasks.
- We use CCTV and audio recording to make sure the School site is safe. CCTV is not used in private areas such as changing rooms and toilets.
- We may need to report some of your information to the government. For example, we may need to tell the local authority that you attend the School or let them know if we have any concerns about your welfare.
- Depending on where you will go when you leave us we may need to provide your information to other schools, colleges and universities or potential employers. For example, we may share information about your exam results and provide references. We may need to pass on information which they need to look after you.
- When you take public examinations (e.g. GCSEs) we will need to share information about you with examination boards. For example, if you require extra time in your exams.
- We may need to share information with the police or our legal advisers if something goes wrong or to help with an inquiry. For example, if one of your classmates is injured at School or if there is a burglary.
- We may share some information with our insurance company to make sure that we have the insurance cover that we need.
- We may share your academic and (where fair) your behaviour records with your parents, education guardian or agent so they can support your schooling.
- We will only share your information with other people and organisations when we have a good reason to do so. In exceptional circumstances we may need to share it more widely than we would normally.
- We will monitor your use of email, the internet and mobile electronic devices e.g. mobile phones. This is to check that you are not misbehaving when using this technology or putting yourself at risk of harm. If you would like more information about this, you can read the Acceptable use of IT and email Policy or speak to your Parent/Carer or Academic Tutor.
- We may use photographs or videos of you for the School's website and social media sites to show prospective students what we do here and to advertise the School. We may continue to use these photographs and videos after you have left the School (in certain circumstances we may ask you or your parents for consent to use a specific image).

- Sometimes we use photographs and videos for teaching purposes.
- We may send your information to, or store your information in, other countries where:
    - we store information on computer servers based overseas; or
    - we communicate with you or your parents when you are overseas (for example, during the summer holidays if you or your parents live in a different country). The European Commission has produced a list of countries which have adequate data protection rules. The country that we are sending your information to might not be on the list which means that it might not have adequate rules.
- We may keep your contact details when you leave so we can find out how you are getting on and to let you know about what is happening at the School. For example we may send you information by post or email, about events and activities taking place (including fundraising communications and events).

If you have any concerns about any of the above, please speak to your Academic Tutor..

What do we do with your personal information?

The Data Protection Officer is the person responsible at our School for managing how we look after personal information and deciding how it is shared. The Data Protection Officer can be contacted at **david.coy@london.anglican.org** and can give you more information about your rights.

Like other organisations, we need to keep your information safe, up to date, only use it for what we said we would, destroy it when we no longer need it and most importantly – treat the information we get fairly.

For how long do we keep your information?

We keep your information for as long as we need to in order to educate and look after you.
We will keep some information after you have left the School, for example, so that we can find out what happened if you make a complaint.

In exceptional circumstances we may keep your information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under data protection law. We can keep information about you for a very long time or even indefinitely if we need this for historical, research or statistical purposes. For example, if we consider the information might be useful if someone wanted to write a book about the School.

Please refer to our Data Storage and Retention Policy for further information about what type of information we hold.

Our legal grounds for using your information

- As a School we have to comply with various laws and this entitles us to use your information where necessary. For example, we have to make sure that we take care of you properly.
- Unless this would be unfair to you, we have a legitimate interest in using your information in order to:
    - educate you and others;
    - look after your welfare and the welfare of others; and
    - promote and develop the School so that it continues to be successful.
- If you object to us using your information where we are relying on our legitimate interests as explained above, please speak to the Data Protection Officer.
- We also use your information in order to provide education, which is in the public interest.
- If something goes wrong, we may need to use your information in connection with legal disputes

- We have an agreement with your parents to educate and look after you. We are allowed to use information about you where this is necessary under this agreement.
- We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Please contact the Data Protection Officer.
- We are allowed to use your information in an emergency, for example, if you require urgent medical attention.
- We may use information about you if we need this for historical, research or statistical purposes.

What decisions can you make about your information?

From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights. Your rights are as follows:

- if information is incorrect you can ask us to correct it.
- you can also ask what information we hold about you and be provided with a copy. We will also give you extra information, such as why we use this information about you, where it came from and what types of people we have sent it to.
- you can ask us to delete the information that we hold about you in certain circumstances. For example, where we no longer need the information.
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer.
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy.

Further information and guidance

This notice is to explain how we look after your personal information. Please speak to the Data Protection Officer if:

- you object to us using your information for marketing purposes e.g. to send you information about school events; or
- you would like us to update the information we hold about you; or
- you would prefer that certain information is kept confidential.

If you have any questions you can ask your Parent/Carer about how it works in our School.

You can ask your Parent/Carer to speak to the Data Protection Officer or speak to him yourself. Alternatively, you can ask your parents to speak to us on your behalf.

If you consider that we have not acted properly when using your personal information, you can contact the Information Commissioner's Office: www.ico.org.

Appendix 5 - Student and Parent Privacy Notice

Student and parent Privacy Notice

How we use student and parent information

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 (Appendix 5)	
Version	Last updated: 03.03.2019	

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you and your child(ren), 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 it, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, the Richmond upon Thames School are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO), David Coy, Email: david.coy@london.anglican.org

Why do we collect and use student and parent information?

We collect and use the student and parent information under the Education Act 1996.
https://www.gov.uk/education/data-collection-and-censuses-for-schools
We use the student and parent data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral and medical care
- for safeguarding and student 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

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

- Personal information (such as name, unique student number and address, parents national insurance number)
- Any relevant medical information (such as NHS information, health checks, physical and mental health care, immunisation program and allergies)
- Special educational needs information (such as EHCPs, statements, applications for support, care or support plans)
- Safeguarding information
- Exclusions and behavioural information
- Assessment information (such as data scores, tracking, and internal and external testing)
- 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)
- Photographs (for internal safeguarding and security purposes, school newsletters, media and promotional purposes)
- CCTV images
- Payment details
- Biometric data
- Genetic data

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

The lawful basis on which we use this information
Our lawful basis for collecting and processing student information 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 student information 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 students can be found here [link to record of processing].

Where we have obtained consent to use students' 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 students' 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 student 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 student consent to the provision of information
- ensures schools are protected from any legal challenge that they are breaching a duty of confidence to students
- helps to ensure that returns are completed by schools

Collecting student information

Whilst the majority of student 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 student information to us or if you have a choice in this.
Where we have obtained consent to use students' 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.

Storing student data

We hold student data for 6 years following a student's last entry which would be when they reach **23 years of age** (as we are an 11-16 school).

We hold student data whilst the child remains at The Richmond upon Thames School. The file will follow the student when he / she leaves The Richmond upon Thames School/will be retained until the Date of Birth of the student + 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 here to our Data Storage and Retention policy for further information.

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.

Who do we share student information with?

We routinely share student information with:

- schools that the student's attend after leaving us
- our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- the Department for Education (DfE)
- School nurse
- The student'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

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.

Why we share student information?

- We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.
- We share students' 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 students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

- We are required to share information about our students with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Students) (England) Regulations 2013.
- We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

Youth support services

What is different about students aged 13+?
Once our students reach the age of 13, we also pass student 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 / 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 / student once he/she reaches the age 16.
For more information about services for young people, please visit our local authority website: www.richmond.gov.uk

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.

The National Student Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students 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 students 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 Students) (England) Regulations 2013.

To find out more about the student information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information.

The department may share information about our students 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 student 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 student information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-student-database-requests-received

To contact DfE
https://www.gov.uk/contact-dfe

Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, parents and students have the right to request access to information about them that we hold through a Subject Access Request. To make a request for your personal information, or be given access to your child's educational record, please contact our DPO - David Coy, Email: david.coy@london.anglican.org

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. David Coy, Email: david.coy@london.anglican.org

Parents/carers also have a legal right to access their child's educational record. To request access, please contact: David Coy, Email: david.coy@london.anglican.org - Data Protection Officer.

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

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

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. [insert details here]

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

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

Contact us

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

Email: david.coy@london.anglican.org

Staff Privacy Notice

How we use Staff information

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 (Appendix 6)	
Version	Last updated: 03.03.2019	

1 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, 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. It if, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, **the Richmond upon Thames School** at **Egerton Road, Twickenham, TW2 7SL** are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO), **David Coy**.
Email: **david.coy@london.anglican.org**

1.1 The categories of staff information that we collect, hold and share

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.

1.2 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 students
- 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
- Support the work of the School Teachers' Review Body
- to assess the quality of our services
- to comply with the law regarding data sharing

1.3 The lawful basis on which we use this information

Our lawful basis for collecting and processing staff information 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 found here[link to record of processing].

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 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.

4.1 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 here to our Data Storage and Retention Policy for further information.

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.

4.2 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 eg, HR, payroll, employee benefit schemes
- Financial organisations eg 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.

4.3 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.

4.3.1 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

4.3.2 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.

We are required to share information about our staff with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

5 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 Student 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

6 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: **David Coy.**
Email: **david.coy@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

7 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. **David Coy**.
Email: **david.coy@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

8 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: **David Coy**.
Email: **david.coy@london.anglican.org**

Appendix 7 - Trainees' Privacy Notice

Privacy Notice for Trainees

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 (Appendix 7)	
Version	Last updated: 03.03.2019	

RTS School 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. It if, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, the Richmond upon Thames School, are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO), **David Coy**.
Email: **david.coy@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 staff 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 students
- 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 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 found here[link to record of processing].

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 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 here [link] to our Data Storage and Retention Policy for further information.

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:

- 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 staffing 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, **David Coy.**
Email: **david.coy@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: **David Coy.**
Email: **david.coy@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: **David Coy**.
Email: **david.coy@london.anglican.org**

Appendix 8 - Trustees' Privacy Notice

Privacy Notice for Trustees

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 (Appendix 8)	
Version	Last updated: 03.03.2019	

How we use Trustee Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as trustees 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. It if, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, the Richmond upon Thames School are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO), **David Coy, Email: david.coy@london.anglican.org**

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)
- details of your qualifications, skills, and experience for skills audit purposes;
- details of your bank account and national insurance number for reimbursement of expenses
- 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 trustee
- Your attendance and visits to the school in your role as a trustee
- 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.

Why we collect and use this information

The purpose of collecting and processing this data is to:

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

The lawful basis on which we use this information

Our lawful basis for collecting and processing staff information 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 organisation (includes religious, political or philosophical organisations and trade unions)
- (i) It is in the public interest.

A full breakdown of the information we collect on trustees can be found here [link to record of processing].

Where we have obtained consent to use trustees 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.

Collecting trustee 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 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.

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 trustee 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 our Data Storage and Retention Policy for further information.

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.

Who we share information with

We routinely share staff 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.

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.

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 trustees 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

Requesting access to your personal data and your Data Protection Rights
Under data protection legislation, trustees 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: **David Coy.**
Email: **david.coy@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

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: **David Coy.**
Email: **david.coy@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

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: **David Coy**.
Email: **david.coy@london.anglican.org**

Appendix 9 - Supply/Contractors/Consultants Privacy Notice

Privacy Notice for supply contractors/ consultants

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 (Appendix 9)	
Version	Last updated: 03.03.2019	

How we use Supply, Consultant and Contractor Information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you, 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 it, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, CofE School at [address] are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO): **David Coy.**
Email: **david.coy@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 staff information 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 found here[link to record of processing].

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 or 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 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 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 here [link] to our Data Storage and Retention Policy for further information.

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 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: **David Coy**.
Email: **david.coy@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: **David Coy**.

Email: **david.coy@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, **David Coy.** Email: **david.coy@london.anglican.org**

Appendix 10 - CCTV Policy

CCTV Policy

Responsibility	Finance and Resources Committee	
Status	Statutory	
Ratification date	15 12 2020	
Review cycle / date	2	Autumn 2022
Reference	013 Appendix 10	
Version	Last updated: 03.03.2019	

Purpose

- The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at The Richmond upon Thames School (the School). It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV system (the System).
- The System is administered and managed by the School, who act as the Data Controller. This policy will be subject to review from time to time, and should be read with reference to the School's Data Protection Policy and Privacy Notice. For further guidance, please review the Information Commissioner's CCTV Code of Practice (https://ico.org.uk/media/1542/cctv-code-of-practice.pdf).
- All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds.
- The School's CCTV cameras are located in various locations internal and external throughout the School Premises The School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

Objectives of the System

- To protect students, staff, volunteers, visitors and members of the public with regard to their personal safety.
- To protect the School buildings and equipment, and the personal property of students, staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the School site and deliveries and arrivals, including car parking.
- To monitor staff and contractors when carrying out work duties.
- To monitor and uphold discipline among students in line with the school's behaviour policy.

Positioning

- Locations have been selected that the School reasonably believes require monitoring to address the stated objectives.
- Adequate signage has been placed in prominent positions to inform staff and students that they are entering a monitored area.
- No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.
- No images of public spaces will be captured except to a limited extent at site entrances.

Maintenance

- The CCTV System will be operational 24 hours a day, every day of the year.
- The System Manager (defined below) will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.
- The System will be checked and (to the extent necessary) serviced no less than annually.

Supervision of the System

- Staff authorised by the School to conduct routine supervision of the System may include the Facilities Team staff.
- Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

Storage of Data

- The day-to-day management of images will be the responsibility of Andy Pelton, Facilities Manager, who will act as the System Manager, or such suitable person as the System Manager shall appoint in his absence.
- Images will be stored for 4 weeks, and automatically overwritten unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.
- Where such data is retained, it will be retained in accordance with the Act and our Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

Access to Images

- Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).
- Individuals also have the right to access personal data the School holds on them (please see the School's Privacy Notice and Data Protection Policy), including information held on the System, if it has been kept.
- The School will require specific details including at least to time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.
- The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:
    - Where required to do so by the Head Teacher, the Police or some relevant statutory authority;
    - To make a report regarding suspected criminal behaviour;
    - To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
    - To assist the School in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;
    - To data subjects (or their legal representatives) pursuant to an access request under the Act;
    - To the School's insurance company where required in order to pursue a claim for damage done to insured property; or
    - In any other circumstances required under law or regulation.

  Where images are disclosed a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images

viewed and a crime incident number (if applicable). Where images are provided to third parties, wherever practicable steps will be taken to obscure images of non-relevant individuals.

Other CCTV systems

- The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this is in line with the objectives of the School's own CCTV policy and/or its Behaviour Policy.

Complaints and queries

- Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the Finance Director, Priti Saund. For any other queries concerning the use of your personal data by the School, please see the School's Privacy Notice.

Confirmation of Receipt of the Data Protection Policy

Name:

Date of joining school:

Post:

Date of induction:

Name and designation of member of staff responsible for induction:

I confirm that I have reviewed and read the school Data Protection policy.

Signature: _____

Name: _____

Date: _____

Please sign and return this form to the Designated Safeguarding Lead.