Finchley Catholic High School

Data protection policy

Approved by:		**Date:** May 2018
Last reviewed on:	May 2016	
Next review due by:	May 2020	

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection and Safeguarding Policy
- Staff Acceptable Use Policy
- Staff Code of Conduct

Contents

……

About this policy

The School holds Personal Data about current, past and prospective students, parents, employees and others with whom the School communicates. Personal Data may be recorded on paper or stored electronically.

This Policy and other documents referred to in it set out the basis on which the School will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

This Policy does not form part of any employee's contract of employment and may be amended at any time.

1. Aims

Finchley Catholic High School ('the School', 'we', 'us', 'our') aims to ensure that all Personal Data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR),the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill and associated legislation.

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

2. Legislation and guidance

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

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Functions of the School	The provision of education and any pastoral, business, administrative, community or similar activities associated with that provision.
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. The School is the Data Controller of all Personal Data used for carrying out its functions.
Data processor	A person or other body, other than an employee of the data controller, who processes Personal Data on behalf of the data controller.
Personal Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

4. The data controller

Our School processes Personal Data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

5. Roles and responsibilities

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

5.1 Governing body

The governing body 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 and compliance wih this policy and the Relevant Data Protection Laws. The DPO will monitor our compliance with data protection law, and develop related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body 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 Sue Murphy and is contactable via info@finchleycatholic.org.uk

5.3 Headteacher

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

5.4 All staff

Staff are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy by School staff may result in disciplinary or other action.

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
    - If they have any doubt as to whether any processing exceeds the purposes for which that data were originally collected
    - If they are unsure whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected.

6. Data protection principles

The GDPR is based on data protection principles that anyone processing Personal Data for or on behalf of 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 and in an appropriate way
- 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, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will keep a record of all data processing activities and must be able to demonstrate compliance with these principles and the wider requirements of data protection law.

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 or of another person 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, in particular where the individual is a child)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

Where a type of Data Processing is likely to pose a high risk to individuals' rights and freedoms, the School will carry out an appropriate Privacy Impact Assessment.

For special categories of Personal Data, the individual's explicit consent to processing of those data must be obtained unless the processing:

- is necessary for the purposes of carrying out the obligations and exercising specific rights of the School or of the individual in the field of employment and social security and social protection law;
- is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;
- relates to Personal Data which are manifestly made public by the individual;
- is necessary for reasons of substantial public interest; or
- is necessary to protect the vital interests of the individual.

Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK or EU law states that processing must take place.

7.2 Consent of adults and organisations

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

Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the School) or a positive action demonstrating consent. Any requests that the School makes for consent must be in clear language.

An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the School requests consent.

7.3 Consent of children and young people

Parental consent to Data Processing must be obtained for pupils or other children younger than 13 years of age.

A young person aged 13 or over is able to give or revoke consent (unless they do not have capacity).

Where consent is required from a young person aged 13 or over the requirements in relation to consent, as set out for adults, still apply and the information in relation to such consent must be made clear to the young person.

7.4 Limitation, minimisation and accuracy

We will only collect Personal Data for specified, explicit and legitimate reasons. This may include data we receive directly from a an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, the local authority or other public bodies, business suppliers or service providers, professional advisers and others).

The School will only process Personal Data for the specific reasons set out in Appendix 2 or for any other reasons specifically permitted by Relevant Data Protection Law. 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.

We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

It is the responsibility of staff to ensure that Personal Data is accurate and kept up to date. Further, parents and anyone who provides Personal Data should also inform the School as soon as possible if there is any change to their Personal Data.

Staff must only process Personal Data where it is necessary in order to do their jobs.

We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take reasonably steps to destroy, or erase from our systems, all data which is no longer required. We will be guided by the Information records Management Society guidance in respect of decision making concerning the retention of Personal Data.

8. Notifying individuals

If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

- the identity and contact details for the School and its Data Protection Officer;
- the purpose or purposes for which we intend to process those Personal Data as well as the legal basis for the processing;
- where the processing is necessary for the purposes of legitimate interests, the legitimate interests pursued;
- the recipients or categories of recipients of the Personal Data;
- where applicable, the fact that the School intends to transfer the Personal Data to a third country;
- the period for which the Personal Data will be stored;
- the existence of the rights of the Data Subject;
- where the processing is based on consent, the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of Personal Data is a statutory or contractual requirement and the possible consequences of failure to provide such data;
- the existence of any automated decision-making, including profiling.

If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information above at the following times:

- within one month of receiving the Personal Data;
- if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;
- if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

A notification in the form of a Privacy Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

We will also inform individuals whose Personal Data we process that the School is the data controller with regard to those data and who the Data Protection Officer is.

9. Using data processors

The School retains the right to engage by written contract any person or organisation, who is not a member of School staff, to process Personal Data on our behalf.

Data Processors must:

- assist the School in upholding individuals' data protection rights;
- only act in accordance with the School's instructions and authorisation;
- maintain a written record of processing activities carried out on behalf of the School and provide this to the School within a reasonable period following request;
- notify the School of Personal Data Breaches without undue delay and maintain a register of breaches;
- comply at all times with the terms of any agreements with the School and with their responsibilities under Relevant Data Protection Law;
- satisfy the School, within a reasonable period following request, of their compliance with the terms of their agreement with the School.

10. Sharing Personal Data

We may share Personal Data we hold with staff at the School.

We will not normally share Personal Data with third parties, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our property, staff, customers or others at risk. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.
- In order to enforce or apply any contract with the individual or other agreements, for example:
    - We need to liaise with other agencies – we will seek consent as necessary before doing this
    - Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
        - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
        - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any Personal Data we share
        - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- We will also share Personal Data with law enforcement and government bodies where we are **legally required** to do so, including for:
    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders

- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as Personal Data is sufficiently anonymised or consent has been provided

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

We may also share Personal Data we hold with selected third parties for the purposes set out in Appendix 2.

10.1 Where we share Personal Data to a country or territory outside the European Economic Area

Individuals have particular rights with regard to transfers of their Personal Data outside the European Economic Area ('EEA'). Circumstances in which the School may need to transfer data outside the EEA might include use of IT services hosted overseas, arrangement and administration of School trips and cultural exchange projects.

Subject to the requirements in Clause 10 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

We may transfer any Personal Data we hold to a country outside the EEA provided that:

- the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and
- any transfer to a country or countries outside the EEA is subject the escalation procedure below.

Before a transfer of Personal Data is made outside the EEA, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

- confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country;
- standard data protection Clauses adopted by the European Commission in accordance with Relevant Data Protection Law must be included in relevant documentation;
- ensuring explicit consent is given by the Data Subject to the proposed transfer after having been informed of the possible risks of such transfer;
- confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;
- confirmation that the transfer is necessary for important reasons of public interest;
- the Data Protection Officer must authorise the transfer.

11. Requests for information

Requests for information may take the following forms:

- Requests for education records
- Freedom of information requests
- Subject access requests

Where a person with parental responsibility requests information about a child's educational records then these should be provided.

11.1 Parental requests to see the educational record

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

Where the School needs to comply with a court order this may over-ride any such request.

11.2 Freedom of information requests

If a person makes a request for information under the Freedom of Information Act then the information should usually be provided unless there are some specific concerns about disclosing the information.

Common concerns in the School context may be that information relates to other people, is confidential or legally privileged.

There is extensive guidance on the ICO website. If a freedom of information request is made and there are any concerns about disclosing information then the Data Protection Officer should be contacted.

11.3 Subject access requests

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

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

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

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

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

11.4 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 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our School may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

11.5 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 manifestly unfounded or excessive. In particular, we will consider whether it:

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

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

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

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

12. Rights of the individual

We will process all Personal Data in line with individuals' rights, in particular their rights to:

- be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;
- receive confirmation as to whether your Personal Data is being processed by us;
- access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. School employees who receive a written request should forward it to their senior leader and the Data Protection Officer immediately;
- have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the School
- object to Data Processing on grounds relating to his or her particular situation unless the School demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and
- Not to be subject to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them) unless the decisions is based on the individual's explicit consent
- restrict processing of data if one of the following circumstances applies:

  a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data;

  b) the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

  c) the controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

  d) the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

  Where processing has been restricted, as above, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State and the data subject shall be informed.

  Where processing is restricted, as above, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or the United Kingdom;

  an individual who has obtained restriction of processing shall be informed by the School before the

restriction of processing is lifted;

- receive data concerning the individual, which he or she has provided to the School and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the School;
- Ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances);
- Withdraw their consent to processing at any time;
- 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;
- Prevent processing that is likely to cause damage or distress.

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.

The School may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

The School shall provide information on action taken on a request under Clause 12 to the individual within one month of receipt of the request unless the School deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
- We will also verify the identity of the person making the request by whatever reasonable means are considered appropriate.

Our employees will refer a request to their senior leaders and the Data Protection Officer for assistance in difficult situations. Employees shouldn't feel pressured into disclosing information if they have concerns about disclosing it and should refer any questions to a senior leader or the Data Protection Officer.

13. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

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

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

Parents/carers and pupils have the right to choose not to use the School's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a pre-loaded card for each transaction if preferred.

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

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

Where staff members or other adults use the School's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object.

Staff and other adults can also withdraw consent at any time, and the School will delete any relevant data already captured.

14. CCTV

We use CCTV in various locations around the School site to ensure it remains safe. We adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. CCTV footage CCTV footage will not be kept for longer than one month.

Any enquiries about the CCTV system should be directed to the School Business Manager.

15. Photographs and videos

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

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

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

Uses may include:

- Within School on notice boards and in school magazines, brochures, newsletters, etc.
- On the School website
- 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.

16. 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

17. Data security and storage of records

We will take appropriate security measures to 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.

We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality: only people who are authorised to use the data can access them;
- Integrity: Personal Data should be accurate and suitable for the purpose for which they are processed;
- Availability: authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the School's central computer system instead of on individual computers, tablets or other media.

Security procedures include:

- Any stranger seen in entry-controlled areas should be reported
- 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
- When disposing of paper documents they should be shredded. Digital storage devices should be professionally processed and physically destroyed when they are no longer required.
- Where personal information needs to be taken off site, staff must sign it in and out from the School office
- Passwords that are at least 8 characters long containing letters and numbers are used to access School computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their computers, tablets or other devices when left unattended
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment (see our Acceptable Use Policy)
- Where we need to share Personal Data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

All School staff must:

- assist the School in upholding individuals' data protection rights;
- only act in accordance with the School's instructions and authorisation;
- notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches
- comply at all times with the terms of any agreements with the School and with their responsibilities

under Relevant Data Protection Law;

- satisfy the School, within a reasonable period following request, of their compliance

18. 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.

19. Personal Data breaches

The School will make all reasonable endeavours to ensure that there are no Personal Data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

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

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

20. Training

All staff and governors 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.

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

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

Where appropriate, we will notify individuals of those changes by mail or email.

Appendix 1: Personal Data breach procedure

This procedure is based on guidance on Personal Data breaches produced by the ICO.

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

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the School's computer system (in a register of Personal Data breaches).
- 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 Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

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

APENNDIX 2: Data Processing Activities

Type of data – to be GROUPED BY PURPOSE	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Contact details	Parents/ guardians Pupils Next of kin	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare School trips and activities management Insurance Supporting learning Monitoring and reporting on pupils' progress Providing appropriate pastoral care Health and safety Employment Provision of paid services including music tuition	Consent; Vital Interests; Public Interest; Contractual Performance	Teaching, support and administrative staff Third parties appropriately chosen by the Trust The local authority and other state bodies Appropriate community services Youth support services Local authority Department for Education (DFE) Third parties designated by the DFE Exam Boards	Until the pupil leaves his/or her Trust academy Until the pupil reaches 25 years of age
Medical information	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care Health and safety	Vital Interests; Public Interest	Teaching, support and administrative staff; School nurses; The NHS	Until the pupil leaves his/or her Trust academy
Special educational needs	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care Health and safety School trips and activities management Supporting learning	Vital Interests; Public Interest	Teaching, support and administrative staff; School nurses; The NHS Third parties appropriately chosen by the Trust Appropriate community services Youth support services Local authority	Until the pupil leaves his/or her Trust academy
Religious belief	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare School trips and activities management Providing	Public Interest	Teaching, support and administrative staff Third parties appropriately chosen by the Trust	Until the pupil leaves his/or her Trust academy

Type of data – to be GROUPED BY PURPOSE	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
			appropriate pastoral care For purposes of the PREVENT scheme			
Sexual orientation						
Ethnic group	Pupil	Electronic storage Written correspondence	Monitor pupil progress	Securing equality of opportunity and ensuring quality of provision	Teaching, support and administrative staff Local Authority Data analysis providers	7 years after student leaves school
Disciplinary history	Pupils	Electronic storage Written correspondence	Monitor pupils progress, social and academic development Provide appropriate support and intervention as required Evidence base for any exclusions	Securing appropriate support for individuals where needed. Evidence for any disciplinary hearings as required eg. exclusions	Teaching, support and administrative staff Parents Local authority Data analysis providers	7 years after student leaves school
Vocational learning and qualifications	Pupils	Electronic storage Written correspondence	Analysis of school's performance via curriculum areas, pupil groups, individuals and key stages	Implementing requirements of Education acts and Instructions from DFE	Individual pupils of the school Local Authority and DFE Data analysis provides Ofsted The Diocese	7 years after student leaves school
Attendance history	Pupils	Electronic storage Written correspondence	Track individual and pupil group attendance Provide information for reports as required	Legal requirements for pupils to attend school on a regular basis	Parents Local Authority Census returns	7 years after student leaves school
National curriculum examination results	Pupils	Electronic storage Written correspondence	Analysis of school's academic performance via individuals, pupil groups, key stages and curriculum areas	Implementing requirements of Education act and instructions from DFE	Individual students Local authority DFE Data analysis providers Ofsted The Diocese	7 years after student leaves school
Photographs	Pupils Staff Community Governors	Electronic storage Hard copies/archives Website	Evidence of the life of the school Population of school's management Information system Celebrations Newsletters/ Magazines/Website	Permission given by individuals	Visitors to website and school Readers of school magazine/newsletters	Unknown

Type of data – to be GROUPED BY PURPOSE	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
CCTV footage	All visitors to the school	Electronic	Supporting school and health & safety	Safeguarding of Community	Identified and trained school staff	1 month
Family information	Pupils	Electronic storage Written correspondence	Supporting effective Communication between home and school	Safeguarding of students	Teaching, support and administrative staff	Until pupil leaves school
Court orders	Pupils at school and their families	Electronic storage Written correspondence	Safeguarding of individual pupils Effective pastoral care of pupils	Adherence of court orders	Appropriate school staff Identified other adults eg. Social Workers, EWD etc.	Until court order expires
Destination after leaving school	Pupils	Electronic storage Written correspondence	Compliance with legal requirements Identify trends Identify appropriate IAG for students	Compliance with requirements	Appropriate school staff and Governors School Census DFE Local Authority	Annual
Careers guidance	Pupils	Electronic storage Written correspondence	Ensure appropriate and high quality IAG is available for all students	Compliance with DFE requirements	Students and their parents	Annual
Education						
School Trips	Pupils and school staff	Electronic storage Written communication	Health & Safety compliance Legal compliance Information for parents Effective school communication and administration	Insurance and legal compliance Support of home/school communication	Insurance providers Local Authority Students Parents School staff	Annual
Afterschool Clubs	Pupils and school staff	Electronic storage Written communication	Secure high quality enrichment and extra curriculum opportunity for pupils Health & Safety reasons	Safeguarding of students	School staff Students Parents Wider school community	Annual
Employment and Remuneration Details	School staff	Electronic storage Written communication	Adherence to employment legislation Monitoring of school budget Securing high quality provision within the school	Employment law	The Diocese School payroll providers Individual staff Governors School Census	Updated annually
Child Welfare and Safeguarding	Pupils	Electronic storage Written correspondence	To Safeguard the young people attending this school Contribute to any child protection/safegua	Safeguarding of community and beyond	Local Authority Police Social Services MASH referrals	Until student has left the school

Type of data – to be GROUPED BY PURPOSE	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
			rding meetings for other young people as requested			
Free School Meal Eligibility	Pupils	Electronic storage Written correspondence	Ensure those pupils who are eligible are in receipt of free school meals Track these pupils progress to ensure equality of opportunity	Implementing legal requirements	Local Authority School staff as appropriate Data analysis providers Parents	Until student has left the school
First Language	Pupils	Electronic storage Written correspondence	Ensure appropriate support and Intervention for EAL pupils Monitor progress of pupils in accordance with their home language	Ensure equality of opportunity and appropriate educational provision for students	School staff as appropriate Data analysis providers Local Authorities	Until student has left the school
Nationality	Pupils	Electronic storage Written correspondence	Ensure equality of opportunity Monitor progress of all pupil groups to ensure they all make appropriate progress	Equalities legislation	Teaching, support and administrative staff Local Authorities Data Analysis Providers Census	7 years after student leaves school