Bishop Hogarth
Catholic Education Trust

DATA PROTECTION POLICY

Document Management:	
Date Policy Approved:	29 April 2015
Date Amended:	November 2020
Next Review Date:	November 2021
Version:	4
Approving Body:	Finance & Resources Committee

Statement of intent

The Bishop Hogarth Catholic Education Trust is required to keep and process certain information about its staff and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The Trust may from time to time be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, Department for Education, other schools, educational bodies and suppliers.

This policy is in place to ensure all staff, Directors and Governors are aware of their responsibilities and outlines how the Trust complies with the GDPR. This policy ensures that personal information is dealt with properly and securely and in accordance with our legal duties. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1.0 Legal Framework

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 and accords with non-statutory guidance issued by the Department for Education Protection of Biometric Information of Children and Colleges

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

This policy will be implemented in conjunction with the following other school policies:

- Use of Photographic and Video Images Policy
- Information Security Policy
- E Safety Policy
- Acceptable Use Policy
- Freedom of Information Publication Scheme

2.0 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.

3.0 The Data Controller

Our schools processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore the Bishop Hogarth Catholic Education Trust is a Data Controller.

The Trust is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

4.0 Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

5.0 Roles and Responsibilities

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

Board of Directors
The Board of Directors has responsibility for approving the Data Protection and ancillary policies and monitoring compliance. The Board of Directors is the Data Controller and responsible for the appointment of the Data Protection Officer.

Local Governing Committee / Interim Advisory Board
The Local Governing Committee / Interim Advisory Board has overall responsibility for ensuring that their school complies with all relevant data protection obligations.

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 Directors and Trust Senior Leadership with advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Our DPO is **Julian Kenshole** and is contactable at:

Julian Kenshole
Bishop Hogarth Catholic Education Trust
The Headlands
Darlington
DL3 8RW

Email: jkenshole@carmel.org.uk

Tel: 01325 523418

The Chief Executive Officer
The Chief Executive Officer has management and supervision responsibility for the DPO and ensuring that the DPO:

- is involved, closely and in a timely manner, in all data protection matters
- operates independently and is not dismissed or penalised for performing their tasks
- is provided with adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable them to meet their GDPR obligations, and to maintain their expert level of knowledge
- is given appropriate access to personal data and processing activities
- is given appropriate access to other services within your organisation so that they can receive essential support, input or information

Headteachers/Principals

The Headteacher/ Principal of each school acts as the representative of the Data Controller on a day-to-day basis.

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

6.0 The Right to be Informed - Collecting Personal Data

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

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

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

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.

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.

- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

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

The Carmel Professional Training Centre will use the Guidelines for the Retention of Personal Data used by St Mary's University.

7.0 Accountability

The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR - see **Appendix 1**.

The Trust will provide comprehensive, clear and transparent privacy policies

Additional internal records of the school's processing activities will be maintained and kept up-to-date.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:
- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

The Trust will complete Data Protection Impact Assessments where the 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). High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

8.0 Consent

Where we require to lawfully process information we will ensure the following:

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9.0 Sharing Personal Data

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

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

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10.0 The Right of Access (Subject Access Requests) and Other Rights of Individuals

Subject Access Requests

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Requests can be made verbally or in writing.

When responding to requests, we:

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

We will not disclose information if it:

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

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

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority (the ICO) and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

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

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

A copy of the Subject Access Request Form is attached at **Appendix 2**.

Access to Educational Records

The parental right to access their child's **educational records** only applies to **maintained schools** and therefore access to pupil data must be made through a subject access request.

Children and Subject Access Requests

Unlike the parent's right of access to their child's educational record, it is the pupil's right to make a SAR. 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 below the age of 12 are generally not 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 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.

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

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 6.0), 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.

11.0 CCTV and Photographic & Video Images

The recording of images of identifiable individuals constitutes the processing of personal information, so it is done in line with data protection principles.

The Trust notifies pupils, staff and visitors of the purpose for collecting CCTV images via the display of signage.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

The Trust will seek consent for the use of photographic images in line with the Use of Photographic and Video Images Policy. The precautions taken when publishing photographs of pupils, in print, video or on the school website are detailed in this policy.

12.0 Biometric recognition systems

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it (see consent form at **Appendix 3**).

Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), section 27

of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

(a) if the child is being 'looked after' by a local authority[7] or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.

(b) if paragraph (a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide reasonable alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners. The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result of their not participating in an automated biometric recognition system. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

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 (including sixth form students) use the school's biometric system(s), we will also obtain their consent before they first take part in it (see **Appendix 4**), 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.

13.0 Marketing

Direct marketing is a legitimate use of personal information. When we undertake marketing activities we will ensure that we gain consent by:

- using opt-in boxes
- specifying methods of communication (e.g. by email, text, phone, recorded call, post)
- asking for consent to pass details to third parties for marketing and name those third parties
- recording when and how we got consent, and exactly what it covers

We will ensure that our marketing activities adhere to the ICO Direct Marketing Checklist and Direct Marketing Guidance

14.0 Data Security and Storage of Records

We will protect personal data in Accordance with the Trust's **Information Security Policy** and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

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 Trust 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 Trust's **Information Security Policy**.

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

15.0 Publication of Information

The Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

16.0 Training

All staff are provided with data protection training as part of their induction process.

17.0 Monitoring & Review

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 practice. Otherwise, or from then on, this policy will be reviewed **annually.**

Appendix 1

ORGANISATIONAL & TECHNICAL SECURITY MEASURES

Passwords & User Accounts

- Every user of the system has their own unique username.
- We do not use vendor-supplied password defaults for system passwords and other security
- parameters
- Every user of the system has their own unique password, this expires and is changed every
- 30 days.
- All system passwords are a minimum of 8 characters and must include upper and lowercase letters as well as numbers.
- If an unsuccessful log in attempt is made the account is locked and approval is then required to unlock the account.
- All unnecessary passwords and user accounts e.g. default logins for computers are disabled or removed.
- Once a user of the system leaves the organisation their account is disabled and removed.

Physical Security

- All servers are located in a locked server room with restricted access to the key.
- All removable media e.g. USB Memory Sticks, on all computers and servers are restricted from being used.
- All staff laptops are encrypted to prevent unauthorised access in the event of a loss / theft.
- We restrict access to data on a business need-to-know basis
- We restrict access to physical records and data ensuring records are locked away with restricted key access
- We operate a records retention schedule to ensure that we do not keep data longer than is necessary

Network Security

- We install and maintain a firewall configuration to protect data
- We use and regularly update our antivirus software
- We regularly run scans and ensure that software is kept up to date.
- We remain vigilant against ongoing threats and vulnerabilities through a programme of testing and maintenance.
- We monitor access to network resources
- We regularly test security systems and processes
- We maintain and audit an Information Security Policy that includes a defined process to report and investigate data losses.
- We use spam protection on our email platform to help prevent phishing and email based threats

Appendix 2

Subject Access Request Form

General Data Protection Regulations

Part 1 - Person that the information relates to (the data subject).			
Title	Mr Mrs Miss Ms Other:		
Surname		Forenames	
Maiden Name / Former Names			
Date of Birth		Sex	Male Female
Current Address			
Postcode		Telephone No.	
I enclose a copy of one of the following as proof of the identity of the data subject: ☐ Birth Certificate ☐ Driving Licence ☐ Passport If none of these are available please contact the Data Protection Officer for advice on other acceptable forms of identification.			
Part 2 - Is the requested information about you (are you the data subject)?			
No the information is not about me *(go to part 3)* **Yes the information is about me** *(go to part 4)*			
Part 3 - Person (agent) acting on behalf of the data subject.			
Title	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Other:		
Surname		Forenames	
Address			
Postcode		Telephone No.	
What is your relationship to the data subject *(e.g. parent, carer, legal representative)*			
Do you have legal authority to request the data subjects Information?		Yes ☐	No ☐

If the data subject is under 16, do you have parental responsibility for them?	Yes ☐ No ☐
Provide proof that you are legally authorised to act on the data subjects behalf in the form of: ☐ Letter of Authority ☐ Lasting Power of Attorney ☐ Evidence of parental responsibility (where the child lacks understanding) Other *(give details)*	
Provide proof that you are the person authorised to act on behalf of the data subject by enclosing a copy of one of the following: ☐ Birth Certificate ☐ Driving Licence ☐ Passport If none of these are available please contact your Data Protection Officer for advice on other acceptable forms of identification.	

Part 4 - Details of Information being requested.

As to help us deal with your request quickly and efficiently by giving as much detail as possible about the information you want. If possible restrict your request to a particular service, period of time or incident. If necessary continue this section on a separate page.

Information Requested:

Information requested covers	From:	To:
Relevant details to help us locate the information. *(Address at the time, service or department, names of previous contacts etc.)*		

Part 5 - Access to the information.

The Trust is permitted to charge a reasonable fee if your request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information. We will inform you

Do you wish to:	☐ View the information ☐ Be provided with a copy
Copies *(if requested)* **to be:**	☐ Sent to the data subject ☐ Sent to you ☐ Collected
Do you have any special needs when viewing the information or in what format it is provided?	

Part 6 - Declaration

I certify that the information provided on this form is true. I understand that the Trust is obliged to confirm proof of identity / authority and that it may be necessary to obtain further information in order to comply with this subject access request.			
Name			
Signature		Date	
Warning - a person who unlawfully obtains or attempts to obtain personal information is guilty of a criminal offence and is liable to prosecution.			
Part 7 - Before submitting this form please check that you have:			

- ☐ Enclosed proof of the identity of the person the information is about (the data subject)? *(see part 1)*
- ☐ Enclosed proof of authority to act on behalf of the data subject? *(see part 3)*
- ☐ Enclosed proof of your identity if acting on behalf of the data subject? *(see part 3)*
- ☐ Given enough details for us to locate the information you want? *(see part 4)*
- ☐ Signed and dated the declaration? *(see part 6)*
- ☐ Completed all sections? *(part 3 only to be completed by a person acting on behalf of data subject)*

Please submit this form and accompanying documents in writing, either by letter, email or fax to:

Julian Kenshole
Data Protection Officer
Bishop Hogarth Catholic Education Trust
Carmel College
The Headlands
Darlington
County Durham
DL3 8RW

Telephone: 01325 523418
Email: kensholej@bhcet.org.uk
Fax:: 01325 254335

Appendix 3

Dear Parent/Carer

NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION

The school/college wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. This is for the purposes of [*specify what purpose is – e.g. catering, library access, photocopying / printing*].

The use of automated recognition systems has a number of benefits including:

- Speeds up delivery at tills
- Shortens queues
- Enables healthy eating promotions
- Removes the need for cash and improves security and administration

The information from your child that we wish to use is referred to as 'biometric information' (see next paragraph). Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

Biometric information and how it will be used

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their [*fingerprint/iris/palm*]. The school/college would like to take and use information from your child's fingerprint and use this information for the purpose of providing your child with [*specify what purpose is e.g. cashless catering / book & resource lending services / reprographic services (delete as appropriate)*].

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's fingerprint and convert these measurements into a template to be stored on the system. An image of your child's fingerprint is not stored. The template (i.e. measurements taking from your child's fingerprint is what will be used to permit your child to access services.

You should note that the law places specific requirements on schools and colleges when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

(a) the school/college cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above);

(b) the school/college must ensure that the information is stored securely;

(c) the school/college must tell you what it intends to do with the information;

(d) unless the law allows it, the school/college cannot disclose personal information to another person/body – you should note that the only person/body that the school/college wishes to share the information with is CRB Cunninghams – Education Services | Registered in England & Wales No: 1221095 who supplies our biometric systems. This is necessary in order for our supplier to fulfil their contractual obligations.

Providing your consent/objecting

As stated above, in order to be able to use your child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school/college cannot collect or use his/her biometric information for inclusion on the automated recognition system.
You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.
Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. His/her objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The school/college is also happy to answer any questions you or your child may have.
If you do not wish your child's biometric information to be processed by the school/college, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements for children who are not going to use the automated system to [*insert relevant service e.g. cashless catering / book & resource lending services / reprographic services (delete as appropriate)*].

If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent form to the school/college.

Please note that when your child leaves the school/college, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

Yours sincerely

Insert name
Headteacher / Principal *(delete as appropriate)*

Appendix 4

Dear

NOTIFICATION OF INTENTION TO PROCESS BIOMETRIC INFORMATION FOR STAFF & SIXTH FORM STUDENTS

The school/college wishes to use information about you as part of an automated (i.e. electronically-operated) recognition system. This is for the purposes of [*specify what purpose is – e.g. catering, library access, photocopying / printing*].

The information from you that we wish to use is referred to as 'biometric information' (see next paragraph). Under Data Protection legislation we are required to have your explicit consent to process your biometric information for an automated system.

Biometric information and how it will be used

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their [*fingerprint/iris/palm*]. The school/college would like to take and use information from your fingerprint and use this information for the purpose of providing you with [*specify what purpose is e.g. cashless catering / book & resource lending services / reprographic services (delete as appropriate)*].

The information will be used as part of an automated biometric recognition system. This system will take measurements of your fingerprint and convert these measurements into a template to be stored on the system. An image of your fingerprint is not stored. The template (i.e. measurements taking from your fingerprint is what will be used to permit your to access services).

You should note that the law places specific requirements on schools and colleges when using personal information, such as biometric information, for the purposes of an automated biometric recognition system.

For example:

(a) the school/college cannot use the information for any purpose other than those for which it was originally obtained and made known to you (i.e. as stated above);

(b) the school/college must ensure that the information is stored securely;

(c) the school/college must tell you what it intends to do with the information;

(d) unless the law allows it, the school/college cannot disclose personal information to another person/body – you should note that the only person/body that the school/college wishes to share the information with is CRB Cunninghams – Education Services | Registered in England & Wales No: 1221095 who supplies our biometric systems. This is necessary in order for our supplier to fulfil their contractual obligations.

If you give consent to the processing of your biometric information, please sign, date and return the enclosed consent form to the school/college.

If you do not wish your biometric information to be processed by the school/college then we will provide reasonable alternative arrangements to access services.

Please note that when you leave the school/college, or if for some other reason you cease to use the biometric system, your biometric data will be securely deleted.

Yours sincerely

Insert name
Headteacher / Principal *(delete as appropriate)*

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION

Please complete this form if you consent to the school/college taking and using information from your fingerprint as part of an automated biometric recognition system. This biometric information will be used by the school/college for the purpose of identification for the administration of [*cashless catering / book & resource lending services / reprographic services (delete as appropriate)*].

In signing this form, you are authorising the school/college to use your biometric information for this purpose until you either leave the school/college or cease to use the system. If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school/college at the following address:

[*insert address*]

Once you cease to use the biometric recognition system, your biometric information will be securely deleted by the school/college.

Having read guidance provided to me by [*name of school/college*], I give consent to information from the measurement of my fingerprint being taken and used by [*name of school/college*] for use as part of an automated biometric recognition system for the administration of [*cashless catering / book & resource lending services / reprographic services (delete as appropriate)*].

I understand that I can withdraw this consent at any time in writing.

Name: ……..

Signature: ……

Date: ……

Please return this form to: [*insert suitable delivery point and name of school/college*].