



The Bishop Konstant Catholic Academy Trust

Learning Communities, Inspired by Faith

Privacy Notice for Students May 2018



The Bishop Konstant Catholic Academy Trust,
The Zucchi Suite, Nostell Business Estate, Nostell,
Wakefield, WF4 1AB

Telephone: 01924 802285
Email: admin@bkcat.co.uk **Website:** www.bkcat.co.uk



Privacy Notice for Students - How we use information

What is the purpose of this document?

The Bishop Konstant Catholic Academy Trust (“BKCAT”) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your school career with us, in accordance with the General Data Protection Regulation (“GDPR”). It applies to all students.

BKCAT is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice applies to current and former students. It does not form part of any contract.

The categories of student information that we collect, hold and share about you are:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (progress, achievement)
- Relevant medical information
- Special Educational Needs information
- Behavioural Information
- Post 16 learning information

How is your personal information collected?

We typically collect information either directly or indirectly through application forms, examination entries, attendance records, medical records, attainment records, consent forms, computer records, photographs, video, CCTV and other applications.

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use student information to meet legal requirements and legitimate interests set out in the Education Act 1996 and Regulation 5 of the Education Regulations 2013.



GDPR, any information the academy processes fulfils one of the following requirements from Article 6 of the GDPR:

- 1(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- 1(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- 1(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 1(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Where we process special categories of personal data we do so under obligations covered in Article 9 of GDPR:

- 2(g) – the processing is necessary for reasons of substantial public interest.
- Where the above do not apply the academy will seek consent for specific purposes in line with the following Article 6.1.a.
- 1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- This will be done in writing and will clearly define any other uses of personal information and ask for consent for each and every use.

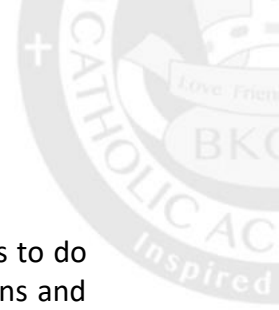
Change of purpose

We will only use student information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Special categories of data

This information includes ethnic group, medical information including health and sickness records and requires higher levels of protection. We will need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- in limited circumstances, with your explicit written consent
- where we need to carry out our legal obligations or exercise rights in connection with your employment
- where it is needed in the public interest, such as for equal opportunities monitoring or for our occupational pension scheme
- less commonly, where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public



Information about criminal convictions

We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided that we do so in line with our data protection policy. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or where we are notified of such information directly by you in the course of you working for us.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

Where information forms part of a **student's** statutory education record, The Education Regulations 2005 SI 2005 No. 1437, the academy will retain the information for 25 years from the child's date of birth. Other information will be retained only where it is required to perform our legal obligations or where it is retained to safeguard and promote the welfare of children and in accordance with our Data Retention Policy.

Who we share student information with

We routinely share student information with:

- schools that the students attend after leaving us
- our local authority
- the Department for Education (DfE)
- School nursing service where appropriate
- NHS where appropriate

Why we share student information

We do not share information about our students with anyone without consent unless we are required to do so by law, or where we have another legitimate interest in doing so. We require third parties to respect the security of your data and to treat it in accordance with the law. We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.



Data collection requirements:

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

Youth support services

Students aged 13+

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

This enables them to provide services as follows:

- youth support services
- careers advisers

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

Students aged 16+

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

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

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

The National Pupil Database (NPD)

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

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.



To find out more about the NPD, go to

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The Department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

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

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

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

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

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

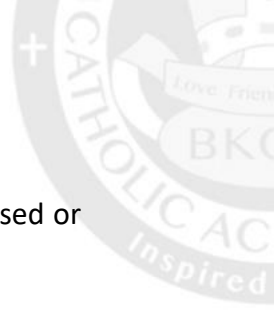
For information about which organisations the department has provided student information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

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

Rights of access, correction, erasure and restriction. Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact **the Data Protection Coordinator at the academy at which your child is registered**. You will not usually have to pay a fee to access your personal information. You also have the right to:

- object to processing of personal data where we are relying on a legitimate interest and the processing is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- request the transfer of your personal information to another party



- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.

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

Contact

If you would like to discuss anything in this privacy notice, please contact:

The Data Protection Officer
The Bishop Konstant Catholic Academy Trust
The Zucchi Suite
Nostell Business Estate
Nostell
Wakefield
WF4 1 AB
Telephone: 01924 802285



Appendix 1: Definitions

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