BOURNE COMMUNITY COLLEGE

Kindness, Respect, Determination

GDPR 2026

Review Date September 2027

Our Aims of the School:

- *To inspire and enable all to make a positive contribution to ourselves, our community and the wider society*
- *Pursue excellence in character and in learning*

Our Vision:

To be the best versions of ourselves

Our Values:

All we do as a community is rooted in our three values

Kindness – a strength of the heart
Respect – a strength of the mind
Determination – a strength of the will

1. Our Commitment

Bourne Community College is committed to protecting all personal and sensitive data for which it holds responsibility as the Data Controller. We handle such data in line with the data protection principles and UK data protection laws.
UK data protection laws comprise the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025
We monitor and implement changes to data protection legislation to remain compliant with all requirements.
The Information Commissioner's Office (ICO) provides guidance on data protection principles: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

2. Roles and Responsibilities

2.1 Data Protection Officer (DPO)

Our DPO is: **Mr Jacques Cariou, Assistant Headteacher**
Contact details: jcariou@bourne.org.uk
The DPO's responsibilities include:

- Advising the school and its employees of their obligations under relevant UK data protection laws
- Monitoring compliance with UK data protection law
- Advising on and assisting with data protection impact assessments
- Acting as a contact point for the Information Commissioner's Office (ICO)
- Acting as a contact point for individuals whose data is processed (staff, students and parents)

However, the school is ultimately responsible for meeting the requirements of the UK GDPR, not the DPO.

2.2 All Staff

All staff must treat all student information in a confidential manner and follow the guidelines set out in this policy. The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

2.3 Headteacher and Senior Leadership Team

The Headteacher and senior leadership team are responsible for:

- Ensuring this policy is implemented and monitored
- Ensuring adequate resources and training are provided to staff
- Supporting the DPO in their role

2.4 Governing Body

The governing body is responsible for:

- Approving this policy
- Ensuring the school complies with data protection legislation
- Receiving regular reports on data protection compliance

3. Registration with the ICO

The school is registered as a data controller with the Information Commissioner's Office (ICO).
Registration Number: Z9881898
Our data processing activities are registered with the ICO. Details are available at: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/
We will notify the ICO of any changes to the type of data processing activities we undertake and amend our registration details accordingly.

4. Personal Data and Special Category Data

4.1 What is Personal Data?

Personal data is information relating to a living individual who can be:

- Directly identified from that information; or
- Indirectly identified from that information in combination with other information

In our school, examples of personal data include:

- Names of staff and students
- Dates of birth
- Photographs of staff and students that are clearly linked to their identity
- Addresses
- National Insurance numbers
- Attendance and behavioural information
- School work and marks
- Exam results

4.2 What is Special Category Data?

Special category data (previously known as sensitive personal data) includes information about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data

- Biometric data (where used for identification purposes)
- Health data
- Sex life or sexual orientation

In our school, examples of special category data include:

- Safeguarding information, including SEN assessments and data
- Medical information, such as medical conditions and GP names
- Free school meal eligibility
- Ethnicity and religion

We process special category data only when we have both a lawful basis under Article 6 of the UK GDPR and an additional condition under Article 9.

5. Data Protection Principles

Under the UK GDPR, personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
4. Accurate and kept up to date
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed
6. Processed in a way that ensures appropriate security of personal data
7. The 7th principle is that the school is responsible for complying with these principles, and must be able to show that it is complying.

6. Lawful Bases for Processing Personal Data

Under the UK GDPR, we can process personal data as long as:

- It's needed to fulfil a contract with the person
- We need to do it to comply with the law
- It will protect someone's 'vital interests'
- We need it to carry out our official functions or for a task in the public interest
- We have the express consent of the person
- We have legitimate interests in the data (as a school, we are unlikely to use this basis)

For most of our data processing activities, we rely on:

- **Legal obligation** - where we are required by law to process the data (e.g., statutory census returns to the DfE)
- **Public task** - where processing is necessary to carry out our official functions as a school (e.g., educating children, maintaining educational records)
- **Vital interests** - where processing is necessary to protect someone's life (e.g., sharing medical information in an emergency)
- **Consent** - only in specific circumstances where none of the other bases apply (e.g., marketing communications, promotional photographs)

We document the lawful basis for each processing activity in our Record of Processing Activities.

7. Consent

We only use consent as a lawful basis when none of the other lawful bases apply. Before choosing consent, we work through the other 5 lawful bases to decide if any apply instead.

7.1 When We Seek Consent

We will seek consent for situations such as:

- Using names, photos, videos or other identifying information about students on the school's website, in the school's newsletter, or other promotional material
- Sending marketing material to prospective parents
- Sending fundraising requests to alumni UK GDPR.

7.2 Requirements for Valid Consent

When seeking consent, we must:

- Offer genuine choice and control
- Be clear and concise, so individuals can understand exactly why we want to process their data
- Allow them to positively opt in
- Be specific – vague or blanket consent is not enough
- Separate consent requests from other terms and conditions
- Tell them how they can withdraw their consent and make it easy for them to do this
- Keep evidence of consent

7.3 Consent from Children

For most consent situations involving students, we will seek parental consent. However, children aged 12 and over can usually provide their own consent if they can understand the data protection implications. We will assess this on a case-by-case basis.

8. Privacy Notices and Transparency

We are transparent about how we process personal data. We communicate our data processing intentions through privacy notices provided to:

- Staff
- Parents/carers

- Students
- Governors

Our privacy notices explain:

- What personal data we collect
- Why we collect it
- The lawful basis for processing
- Who we share it with
- How long we keep it
- Individuals' rights regarding their data

Privacy notices are available on our school website.

9. Sharing Personal Data with Third Parties

We share personal data with third parties only where we have a lawful basis to do so. **We do not rely on consent for most third-party data sharing - instead we use other lawful bases such as legal obligation, public task, or vital interests.**

9.1 Third Parties We Share Data With

Other schools

When a student transfers from Bourne Community College to another school, we share their academic records and data relating to their health and welfare under our legal obligation and public task to ensure educational continuity. This supports a smooth transition and ensures minimal impact on the student's academic progress.

Examination authorities

We share data with examination authorities under our legal obligation to register students for external examinations.

Health authorities

We share data with health authorities under our legal obligation to support public health monitoring, including monitoring and preventing the spread of contagious diseases.

Police and courts

We share data with police and courts when legally required to do so, including during criminal investigations or when ordered by a court.

Social workers and support agencies

UK data protection laws do not prevent or limit us from sharing information to keep children safe. We can share information with the appropriate people if we believe that doing so is likely to support the safeguarding and protection of a child.

We share safeguarding information under our legal obligation and public task to protect children's welfare. We must not share information if it may harm a child or put them at risk of harm.

Educational authorities (including the DfE)

We share data with the Department for Education and other educational authorities under our legal obligation to support government monitoring of the national educational system and to comply with education legislation.

Other third parties

We may also share data with:

- IT service providers and software platforms (as data processors)
- Professional advisers (legal, HR, financial)
- Educational trip providers
- School photographers
- Catering providers
- Transport providers

Where we share data with third parties who act as data processors on our behalf, we ensure appropriate contracts are in place to protect the data.

9.2 Sharing Safeguarding Information

When sharing safeguarding information, we:

- Only share relevant information with individuals, agencies or organisations that have a role in safeguarding the child
- Only provide the information needed to support the provision of services
- Try to engage with the child and/or their family and explain who we intend to share information with, what information we will be sharing and why - but only if it's safe and appropriate to do so.
- We record the reasons for our information sharing decisions, whether we decide to share the information or not.

9.3 International Data Transfers

We do not routinely transfer personal data outside the UK. If we need to do so (for example, for an educational trip abroad or using a cloud-based service with servers outside the UK), we will ensure appropriate safeguards are in place.

10. Data Security

We implement appropriate technical and organisational measures to ensure data security, including:

10.1 Physical Security

- Hard copy data, records, and personal information are stored out of sight and in locked cupboards
- Medical information that may require immediate access is stored securely with the school medical coordinator
- Access to areas containing personal data is restricted to authorised staff only
- Visitors are supervised when in areas where personal data may be accessible

10.2 Digital Security

- All computers and devices are password protected
- Passwords must meet minimum security requirements
- Screens are locked when computers are left unattended
- Encryption is used for storing and transmitting sensitive data

- Regular backups are performed
- Anti-virus and anti-malware software is kept up to date
- Network security measures are in place, including firewalls

10.3 Transporting Data

Staff should not remove personal data from the school site. However, we recognise that some staff may need to transport data for work purposes. When this is necessary:

Paper copies:

- Should be avoided wherever possible
- Must not be on view in public places
- Must not be left unattended under any circumstances
- Must be transported in a secure manner (e.g., in a sealed envelope in a bag)

Digital data:

- Must be stored on encrypted, password-protected USB drives or devices
- Must not be transferred to personal or public computers
- Work should be edited directly from the encrypted device and saved only to that device
- Data should be deleted from portable devices as soon as it is no longer needed

General requirements:

- Staff must ensure printouts are not left in printer trays or photocopiers
- Sensitive information must not be viewed on public computers
- Windows and documents must be properly closed before leaving a computer unattended

Any staff member found to be intentionally breaching these guidelines will be subject to disciplinary action in line with the seriousness of their misconduct.

10.4 Data Protection Impact Assessments (DPIAs)

We carry out Data Protection Impact Assessments when considering new data processing that is likely to result in a high risk to the rights and freedoms of individuals. This includes:

- Implementing new IT systems
- Sharing data in new ways
- Using data for purposes other than those for which it was collected
- Processing special category data on a large scale

11. Data Retention and Disposal

We only keep personal data for as long as necessary for the purposes for which it was collected. We follow retention schedules based on legal requirements and best practice guidance.

Our retention periods are documented in our Data Retention Schedule, which is based on guidance from the Information and Records Management Society (IRMS).

11.1 Secure Disposal

When personal data is no longer required, we dispose of it securely by:

- Shredding paper records containing personal data
- Securely deleting or overwriting digital data
- Using certified disposal services for large-scale disposal
- Obtaining certificates of destruction where appropriate

All staff are responsible for ensuring that:

- Unwanted paper copies of data or personal information are shredded
- Handwritten notes referencing staff or students by name are shredded when no longer needed
- Digital data is permanently deleted when no longer required

12. Individual Rights

Individuals have the following rights regarding their personal data:

12.1 Right to be Informed

Individuals have the right to be informed about how we use their personal data. We provide this information through our privacy notices.

12.2 Right of Access (Subject Access Requests)

Individuals have the right to access their personal data. We have 1 month to comply with subject access requests.

How to make a subject access request:

Requests should be made in writing to:
Mrs A Sharma, Headteacher
Bourne Community College
Southbourne
Emsworth
PO10 8PJ
Email: office@bourne.org.uk

We will ask individuals to complete a Subject Access Request form to help us process the request efficiently. **We do not charge a fee for processing subject access requests** unless the request is manifestly unfounded, excessive, or repetitive.

Information we may withhold:

If a parent asks to see information about their child that relates to child abuse, we can refuse if it wouldn't be in the best interests of the child. If they ask to see education data or social work data, we can refuse if we believe that sharing it would be likely to cause serious harm to the physical or mental health of any individual. We may also withhold information where:

- It would reveal the identity of another person (unless they have consented or it is reasonable to disclose without consent)

- The information is subject to legal professional privilege
- The request is manifestly unfounded or excessive

12.3 Right to Rectification

Individuals have the right to have inaccurate or incomplete personal data corrected. We will respond to requests for rectification within 1 month.

12.4 Right to Erasure

Individuals have the right to request erasure of their personal data in certain circumstances. **However, this right is not absolute.**
We may refuse a request for erasure where we have a legal obligation to retain the data, such as:

- Safeguarding records
- Financial records required for audit purposes
- Examination data
- Records required under education legislation
- Records needed to establish, exercise or defend legal claims

Each request will be assessed on a case-by-case basis.

12.5 Right to Restrict Processing

Individuals have the right to request that we restrict processing of their personal data in certain circumstances, such as when they contest the accuracy of the data.

12.6 Right to Data Portability

Individuals have the right to receive their personal data in a structured, commonly used and machine-readable format, and to transmit that data to another controller, where technically feasible.

12.7 Right to Object

Individuals have the right to object to processing based on legitimate interests or the performance of a public task. We will stop processing unless we can demonstrate compelling legitimate grounds that override the individual's interests.

12.8 Rights Related to Automated Decision Making

Individuals have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. We do not currently use automated decision-making processes.

13. Data Protection Complaints

Under the Data (Use and Access) Act 2025, we must give people a way of complaining to us about how we've handled their personal data, and we must acknowledge the complaint within 30 days and investigate the issue as soon as possible. The UK GDPR: summary (The Key Leaders)

How to make a complaint:

Complaints about data protection should be made in writing to our Data Protection Officer:

Mr Jacques Cariou
Bourne Community College
Southbourne
Emsworth
PO10 8PJ
Email: jcariou@bourne.org.uk

We will:

- Acknowledge your complaint within 30 days
- Investigate the issue as soon as possible
- Provide a written response explaining our findings and any action taken

Complaints to the ICO:

If you are not satisfied with our response, you have the right to complain to the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Website: www.ico.org.uk

13. Data Breaches

We must notify the ICO within 72 hours of a data breach if the breach puts people at risk. We must also keep a record of any personal data breaches, regardless of whether we are required to report them.

14.1 What is a Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data
- Sending personal data to the wrong recipient

- Unauthorised access to personal data
- Alteration of personal data without permission
- Loss of availability of personal data

14.2 Reporting a Data Breach

All staff must report suspected data breaches immediately to the Data Protection Officer (Jacques Cariou)
The DPO will:

- Investigate the breach
- Assess the risk to individuals
- Determine whether the breach must be reported to the ICO (within 72 hours if required)
- Determine whether affected individuals must be notified
- Record the breach in our data breach register
- Take steps to mitigate the breach and prevent recurrence

14.3 Data Breach Register

We maintain a register of all data breaches, including:

- The nature of the breach
- The categories and approximate number of individuals affected
- The likely consequences
- The measures taken to address the breach

14. CCTV

We use CCTV for security purposes and for the protection of students, staff and property. Our use of CCTV is in accordance with our separate CCTV Policy.
CCTV signage is displayed prominently around the school to inform individuals that CCTV is in operation. Information about our CCTV system is included in our privacy notices.

15. Photographs and Videos

We may capture images of staff and students during appropriate times and as part of educational activities.

16.1 Use of Images for Promotional Purposes

We will seek parental consent (or student consent for students aged 12 and over, where appropriate) before using photographs or videos of students for:

- The school website
- School newsletters
- Social media

- Prospectuses and other promotional materials
- Local or national media

16.2 Images for Internal Use Only

We do not require consent for photographs or videos used solely for internal educational purposes, such as:

- Recording school plays or concerts for internal review
- Photographs for internal displays
- Images for student records

These images will not be published externally without appropriate consent.

16.3 External Parties Taking Photographs

External parties (including parents) may not capture images of staff or students during school activities without prior consent from the school. We communicate this policy to parents through our acceptable use policies and event-specific communications.

16. Biometric Data

We must seek parental consent if we process students' biometric data (such as fingerprints for cashless catering). This is required under the Protection of Freedoms Act 2012, separate to UK GDPR requirements.
We will:

- Notify parents before processing biometric data
- Obtain written consent from at least one parent
- Provide alternative arrangements for students whose parents do not consent or who object themselves
- Allow parents or students to withdraw consent at any time
- Delete biometric data when a student leaves the school
-

17. Training and Awareness

We are committed to ensuring that all staff understand their data protection responsibilities.
All staff will receive:

- Data protection training as part of their induction
- Regular refresher training (annually)
- Updates on changes to data protection legislation and school procedures

The DPO will receive appropriate training to maintain their expert knowledge and keep up to date with developments in data protection law.
Governors will receive training on their data protection responsibilities as part of their governance role.

Monitoring and Review

This policy will be reviewed annually by the DPO and governing body, or sooner if there are changes to data protection legislation or our processing activities.
The DPO will conduct regular audits of our data protection practices and report findings to the senior leadership team and governing body.

Dear Bourne Community College

Please could you provide me with the information requested below that I am entitled to receive under the General Data Protection Regulation and Data Protection Act 2018. I require this information so that I can verify the lawfulness of the information that you are processing.

My personal contact details and the list of information that I require from you are as follows:

Requester's Name	
Address	
Email address	
Phone number	
Data Subjects name (name of student)	
Data Subject date of birth	
Specific details of information requested Please be as precise as possible i.e. attendance records, behaviour records, correspondence	
Date period to be covered	

I am aware that if I am requesting this information as a parent/carer of the data subject, I can only request this information before my child's 16th birthday after which time this request is invalid and the data subject will have to make the request themselves.

I agree to you contacting me using the above contact details to verify my authority to make this request and to clarify any of the information I have requested if necessary.

This Subject Access Request is required to be completed by you within one month of receipt of this document.

Signed …… Date ……