BOURNE COMMUNITY COLLEGE

Kindness, Respect, Determination

GDPR 2025

Review Date September 2026

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

General Data Protection Regulation

Our Commitment:

Bourne Community College is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA) . https://ico.org.uk/for -organisations/guide -to -data -protection/data -protection -principles/

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows:

(a) **Consent:** the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for the member of staff's employment contract or student placement contract.

(c) **Legal obligation:** the processing is necessary for the school to comply with the law (not including contractual obligations)

The key member of staff responsible for data protection is mainly Mr Jacques Cariou, Assistant Headteacher and DPO (Data Protection Officer). However, all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.
The school is registered as a data controller with the Information Commissioner's Office (ICO) Reg No Z9881898.

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

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.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about -the -ico/what -we -do/register -of-data -controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive da ta shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

In a school, some examples of personal information include:

- Names of staff and pupils.
- Dates of birth.
- Photographs of staff and pupils that are clearly linked to their identity or other personal information about them.
- Addresses.
- National insurance numbers.
- Attendance and behavioural information.
- Safeguarding information, including SEN assessments and data.
- School work and marks.
- Medical information, such as medical conditions and GP names.
- Exam results.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for -organisations/ guide -to -data -protection/key - definitions/

Under the GDPR, the data protection principles set out the main responsibilities for organisations;

- 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; and
- 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."

Fair Processing / Privacy Notice:
We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and students prior to the processing of individuals' data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for -organisations /guide -to -data -protection/privacy -notices - transparency -and -control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For security purposes and for the protection of students the use of CCTV is in operation, in accordance with the schools CCTV policy.
The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of an individual's data shall first be notified to them.
Under no circumstances will the school disclose information or data:

- that would cause serious harm to the student or anyone else's physical or mental health or condition
- indicating that the student is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the student recorded by the
- student in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the
- information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the student's potential employer or any national body concerned with student admissions.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for -organisations/guide -to -data -protection/principle -7-security/
https://ico.org.uk/for -organisations/guide -to -data -protection/principle -7-security/
https://ico.org.uk/about -the -ico/news -and -events/news -and -blogs/2014/02/privacy - impact -assessments -code -published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or

information about what is held. We shall respond to such requests within 30 days and they should be made in writing to:

Mrs A Sharma Headteacher
Bourne Community College
Southbourne,
Emsworth
PO10 8PJ

There is a proforma that the individual requesting the information will be asked to fill in. This can be found in appendix at the end of this policy.

No charge will be applied to process the request.

Personal data about students will not be disclosed to third parties without the consent of the student's parent or carer, unless it is obliged by law or the best interest of the student. Data may be disclosed to the following third parties without consent:

- **Other schools**
  if a student transfers from Bourne Community College to another school, their academic records and other data that relates to their health and welfare

  will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the student is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the student's academic progress as a result of the move.

- **Examination authorities**
  This may be for registration purposes, to allow the student at our school to sit examinations set by external exam bodies.

- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of students in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**
  In order to protect or maintain the welfare of our students, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- **Right to be Forgotten**
  Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Images of staff and students may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the schools' policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard.The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator Mrs. Murray Brown.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with students.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or student files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or student by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto an encrypted USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the encrypted USB, and saved onto the USB only.
- USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

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 ……