Bourne Education Trust

Data Protection Policy v7.2

June 2021

File:	BET Data Protection Policy	
Author:	R Isaac	
Version:	V7.1 May 2020	Minor amends; additions to S20: definitions
	V7.2 June 2021	Additions/amendments to paragraphs: 5.1 5.7 10.11 10.12 12.8 13.8 14.3 14.4 14.11 15.3 16.4
Date of next review:	May 2023	

Contents

1. Statement of intent

The Bourne Education Trust aims to ensure that personal data about staff members, pupils, parent(s)/carer(s), governors and visitors is collected, stored and processed in accordance with its legal obligations under the General Data Protection Regulation (UK GDPR), and the expected provisions of the Data Protection Act 2018, as set out in the Data Protection Bill.

The schools within the Trust may, from time to time, be required to share personal information about pupils, parent(s)/carer(s) or staff, including volunteers and governors with other organisations, including the Local Authority, other schools and educational bodies, and various commercial organisations with whom they have contracted services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR.

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

2. Legal framework

2.1 This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- Protection of Freedoms Act 2012.

2.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'.

3. Applicable data

3.1 For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including such information as online identifiers, including IP addresses. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4. Principles

4.1 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 – see Section 7: Lawful Processing
- 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.

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

5. Accountability

5.1 This policy applies to all BET staff, members and trustees, and to external organisations or individuals working on behalf of BET or any of its schools. Staff who do not comply with this policy may face disciplinary action.

5.2 The Bourne Education Trust and its schools will implement appropriate technical and organisational measures to ensure that data is processed in line with the principles set out in the GDPR.

5.3 The Bourne Education Trust will provide comprehensive, clear and transparent privacy policies.

5.4 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

5.5 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 individual's and personal data
- Retention schedules
- Categories of recipients of personal data

- Description of technical and organisational security measures
- Details of transfers to other countries, including documentation of the transfer mechanism safeguards in place.

5.6 Each school will implement measures that meet the principles of data protection by design and by default, such as:

- Data minimisation (see Section 20 for definitions)
- Pseudonymisation
- Transparency
- Allowing individuals such as a member of the Local Governing Committee with responsibility for data protection, or a member of the BET central data protection team to monitor processing
- Continuously creating and improving security features.

5.7 Data protection impact assessments (DPIA) will be used before any new system or process using personal data is introduced to assess the risk to personal data (see section 12).

6. Data protection officer (DPO)

6.1 A BET Data Protection team, including one or more DPOs, will:

- Inform and advise each school and its employees about their obligations to comply with the GDPR and other data protection laws
- Monitor each school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting an annual audit, and advising on the required training of staff members.

6.2 The individual(s) appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

6.3 The DPO will report to the highest level of management in the Trust, which is the CEO.

6.4 The DPO will operate independently and will not be dismissed or penalised for performing their task.

6.5 Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6.6 The DPO team can be contacted by email: dpo@bourne.education.

7. Lawful processing

7.1 The legal basis for processing data will be identified and documented within the GDPRiS platform prior to data being processed.

7.2 Under the GDPR, data will be lawfully processed under one of the following conditions:

- The consent of the data subject has been obtained (or the data subject's parent/carer if aged under 13)
- Processing is necessary for:

- Compliance with a legal obligation
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- For the performance of a contract with the data subject or to take steps to enter into a contract
- Protecting the vital interests of a data subject or another person
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.3 Special category personal data will only be processed under one of the special category conditions set out in the GDPR.

8. Consent (where consent is the legal basis for processing)

8.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

8.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

8.3 Where consent is given, a record will be kept documenting how and when consent was given.

8.4 Each school will ensure 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.

8.5 Consent accepted under the DPA 2018 will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

8.6 Consent can be withdrawn by the individual at any time, where this is the lawful basis for processing.

8.7 For data subjects aged under 13, the consent of a parent/carer will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

8.8 For data subjects aged 13 or over, both the data subject's and the consent of a parent/carer will be sought prior to the processing of the child's data, except where the processing is related to preventative or counselling services offered directly to a child. Should there be disagreement between the wishes of a child aged 13-16 and a parent/carer, it will be assumed that consent has not been given.

8.9 If it is the view of the school that a child aged between 13 and 16 does not have the capacity to give consent, then the view of a parent/carer will be acted upon.

8.10 Where consent has already been gained, for example for using a pupil's photograph for display, consent will not be renewed when the pupil reaches 13, but they will be made aware that they can withdraw consent at any time from the age of 13.

9. The right to be informed

9.1 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.

9.2 If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

9.3 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 and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

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

10. The right of access

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

10.2 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.

10.3 The school will verify the identity of the person making the request before any information is supplied.

10.4 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

10.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.7 All requests will be responded to without delay and at the latest, within one month of receipt. Should a subject access request be made during a school holiday, every attempt will be made to respond within the necessary timeframe, but this cannot be guaranteed.

10.8 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, subject to 10.7.

10.9 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 and to a judicial remedy, within one month of the refusal.

10.10 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 and agree, where appropriate, a specific and relevant subset of the information.

10.11 A child's personal data belongs to them, and not the child's parents or carers. For a parent or carer to make a SAR in respect of their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent. Children aged 13 and above are generally regarded to be sufficiently mature to understand their rights and the implications of a SAR. Therefore, most SARs from parents/carers of students aged 13 or over may not be actioned without the express permission of the child.

10.12 The ICO's Subject Access code of practice (v1.2) will be followed.

11. Other data protection rights. Individuals have the right to:

11.1 Withdraw their consent to processing at any time, where consent is the lawful basis for processing.

11.2 Ask for their data to be rectified, erased, the processing restricted or object to the processing of it (in certain circumstances).

11.3 Prevent use of their personal data for direct marketing.

11.4 Challenge processing which has been justified on the basis of public interest.

11.5 Request a copy of agreements under which their personal data is transferred outside the European Economic Area.

11.6 Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).

11.7 Prevent processing that is likely to cause damage or distress.

11.8 Be notified of a data breach in certain circumstances.

11.9 Make a complaint to the ICO (Information Commissioner's Office) https://ico.org.uk/.

11.10 Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

12. Privacy by design and Data Protection Impact Assessments (DPIA)

12.1 The school will act in accordance with the GDPR by adopting a privacy by design approach, implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

12.2 Data protection impact assessments (DPIA) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

12.3 A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

12.4 A DPIA will be used for more than one project, where necessary.

12.5 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.

12.6 The school 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.

12.7 Where a DPIA indicates high risk data processing, the school will consult the BET Data Protection team: dpo@bourne.education who may then seek advice from the ICO as to whether the processing operation complies with the GDPR.

12.8 For any apps, online games, web or social media sites subscribed to by the school for the use of pupils, reference will be made in the DPIA to the ICO's Children's Code to ensure that privacy settings are high by default, geo-location services are turned off by default, and 'nudge' techniques are not used.

13. Data breaches

13.1 The term 'personal data breach' refers to a breach of security that has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

13.2 Headteachers at Bourne Education Trust schools, or their representatives, will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

13.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

13.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

13.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

13.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

13.7 Effective and robust breach detection, investigation and internal reporting procedures are in place at each school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

13.8 Minor, non-reportable breaches, and 'near misses' will be logged in the school's GDPRiS platform for training purposes.

13.9 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

14. Data security

14.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

14.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

14.3 Personal data held in digital form is coded, encrypted or password-protected, both on a local hard drive and on a regularly backed up network drive or cloud storage site.

14.4 Where personal data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. The portable device must either be encrypted or password protected. The use of portable data storage devices is being phased out.

14.5 ‘Memory sticks’ will not be used to hold personal information unless they are password-protected and fully encrypted. Memory sticks and portable data storage devices will be phased out as soon as technically feasible.

14.6 All electronic devices used to store or process personal data are password-protected to protect the information on the device in case of theft.

14.7 Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft or loss.

14.8 Staff and governors will not use their personal laptops, computers or personal email accounts for school purposes without password protection that prevents, for example, family members accessing the data.

14.9 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

14.10 No sharing of passwords will take place under any circumstances. This is potentially a disciplinary matter.

14.11 Emails containing sensitive or confidential information are password-protected or a secure email system such as Egress is used.

14.12 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

14.13 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

14.14 Where personal information that could be considered private or confidential is taken off the premises, for example on a school trip, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping papers/devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

14.15 Before sharing data, all staff members will ensure:

- They are allowed to share it
- That adequate security is in place to protect it
- The recipient of the data has been outlined in a privacy notice.

14.16 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times, or confidential or personal data on display is covered or removed

14.17 The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

14.18 The Bourne Education Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

14.19 The Data Protection Officer is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

15. Publication of information

15.1 The Bourne Education Trust publishes various documents on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information.

15.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

15.3 Schools within the Bourne Education Trust will not publish any personal information, including photos, on its website without the consent of the affected individual, or a parent/carer if aged under 13. Such consent can be obtained on entry to the school with the expectation that it remains in force whilst the pupil is on the school roll.

15.4 When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

16. Processing of still/moving digital images

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

16.2 The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via clearly displayed notices.

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

16.4 All CCTV footage will be kept for no more than 14 days for security purposes; each school's Data Protection Compliance Officer is responsible for keeping the records secure and allowing access to individuals authorised by the Headteacher.

16.5 The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them (see 15.3).

16.6 If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from a parent/carer of the pupil and the pupil if s/he is aged 13 or over.

16.7 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

16.8 CCTV images will be accessible to the minimum necessary number of staff, as identified by the Headteacher of each school.

16.9 BET schools use live streaming of lessons as required for online/remote learning. Live lessons are recorded for safeguarding purposes and to allow pupils to access the materials once the lesson is concluded. The legal basis for this processing is 'public task'. Recordings of lessons are retained only for as long as necessary to deliver the curriculum. Staff are responsible for adhering to UK GDPR when teaching remotely and are required to adhere to strict safeguarding protocols as outlined in the 'Remote Learning' policy.

17. Data retention

17.1 Data will not be kept for longer than is necessary, following the guidance of the Information and Records Management Society, in their School Toolkit: IRMS Schools Toolkit.

17.2 Unrequired data will be deleted as soon as practicable.

17.3 Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

17.4 Paper documents will be shredded or pulped and securely disposed of, and electronic memories scrubbed clean or destroyed to ISO 27001 or equivalent, once the data should no longer be retained.

18. Disclosure and Barring Service (DBS) data

18.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

18.2 Data provided by the DBS will never be duplicated.

18.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

19. Policy review

19.1 This policy is reviewed annually by the Data Protection Officer and the CEO.

The next scheduled review date for this policy is May 2023

Definitions:

Term	Definition
Data controller	A person or organisation that determines the purposed for which, and the manner in which personal data is processed.
Data minimisation	The collection, storage and use of personal data will be limited to that which is relevant, adequate and necessary for carrying out the purpose for which the data is processed.
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller.
Data Protection Officer	The person responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements.
Data subject	The person whose data is held or processed.
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified.
Processing	Obtaining, recording or holding data.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects, in particular to analyse or predict aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	The process of separating personal data from direct identifiers so that identification is not possible without additional information, held separately.
Sensitive personal data (Special Category Data)	Data such as: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious beliefs, or beliefs of a similar nature ▪ Trade Union membership ▪ Physical and/or mental health ▪ Sexual orientation ▪ Criminal convictions.
Transparency	Personal data will only be used for the purposes stated in this policy and the relevant Privacy Notice(s).