Bradford Grammar School

Data Protection Policy

This policy applies to the whole school.

Updated 25 May 2018

1 Policy statement

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of its activities, Bradford Grammar School (the "School") will collect, store and process personal data (both paper based and electronic) about its pupils, parents, suppliers and other third parties, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on the School's behalf. Any serious and/or repeated breach of this policy may result in disciplinary action.

1.3 The School also holds and processes personal data for a wide range of purposes, including:

- purchase and supplier information;
- fundraising;
- charity & voluntary organisation objectives;
- education and training administration; and
- personnel/employee administration.

1.4 This policy and any other documents referred to in it sets out the way in which the School will process any personal data that it collects from data subjects, or that is provided to the School by data subjects or other sources.

1.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.6 This policy sets out rules on data protection and a summary of the legal conditions that must be satisfied when the School obtains, handles, processes, transfers and stores personal data.

2 Data Protection Officer

2.1 The School has appointed the Bursar & Clerk to the Governors as the Data Protection Officer ("DPO") who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the General Data Protection Regulation ("GDPR"). Within the School, each employee has a direct responsibility for ensuring compliance with the GDPR and this policy. This includes ensuring that data is kept securely and not made available to unauthorised parties. The DPO has overall responsibility for compliance with the GDPR and this policy.

3 Definition of data protection terms

3.1 **Data** is information which is stored electronically, on a computer or in certain paper based filing systems.

3.2 **Data Controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. The School is the data controller of all personal data used in its business for its own purposes.

3.3 **Data users** are those employees whose work involves processing personal data. Data users must at all times protect the data that they handle in accordance with this policy and any applicable data security procedures.

3.4 **Data Processors** include any person or organisation that processes personal data on the School's behalf and on its instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the School's behalf.

3.5 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.6 **Data subjects** are living individuals about whom the School holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.7 **Personal data** is data relating to a living individual who can be identified from that data (or from that data and other information in the School's possession). It includes information that is factual, such as information necessary for employment (employee's name and address and details for payment of salary), but it can also be an opinion about that person, their actions or behaviour.

3.8 **Special Categories of Personal Data** (referred to in this policy as sensitive personal data) is information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4 Processing of personal data

4.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2 You may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

4.3 The GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;

- to meet our legal compliance obligations;

- to protect the Data Subject's vital interests;

- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices

5 The principles

5.1 The School shall, so far as is reasonably practicable, comply with the legislation and the principles contained within it to ensure that all data is:

- processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).
- accurate and where necessary kept up to date (Accuracy).
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
- not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- made available to data subjects and data subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

6 Fair and lawful processing

6.1 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the performance of the contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, to protect the vital interests of a data subject or another person or for the legitimate interests of the data controller or the party to whom data is disclosed.

7 Rights of access to information (subject access request)

7.1 Employees have the right of access to information held by the School, subject to the provisions of the GDPR. Any employee wishing to access their personal data should put their request in writing to the DPO using the form in appendix 1. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within one month. The information will be provided to the data subject as soon as is reasonably possible.

7.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

7.3 Any data subjects (not just employees) can make a subject access request. Employees who are asked to deal with a subject access request from a data subject should forward the request to the DPO.

8 Processing for limited purposes

8.1 Personal data may only be processed for the specific purposes notified to the data subject when data was first collected or for any other purposes specifically permitted by the GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which data is processed, the data subject must be informed of the new purpose before any processing occurs and/or if necessary fresh consent should be obtained.

9 Notifying data subjects

9.1 If the School collects personal data directly from data subjects, it will inform them of:

- the purpose or purposes for which the School intends to process that personal data;
- the types of third parties, if any, with which the School will share or to which it will disclose that personal data; and
- the means, if any, with which data subjects can limit the School's use and disclosure of their personal data.

9.2 If the School receives personal data about a data subject from other sources, it will provide the data subject with this information as soon as possible thereafter.

9.3 The School will inform data subjects whose personal data it processes that it is the data controller with regard to that data.

10. Use of CCTV

The School use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the DPO.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages
- As part of historical data (without identities included)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

11 Accurate data

11.1 The School will ensure that the personal data that it holds is accurate and kept up to date. It will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. The School will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

12 Timely processing

12.1 Personal data should not be kept longer than necessary for the purpose. This means that data will be destroyed or erased from the School's systems when it is no longer required.

13 Processing in line with data subjects' rights

13.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw consent to processing at any time;
- receive certain information about the data controller's processing activities;
- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which personal data is transferred outside of the EEA;
- object to decisions based solely on automated processing, including profiling;
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

13.2 There are certain records which are exempt from the rights of access and these include those relating to references given and sought in confidence by the School for the purposes of education, training or employment of a pupil. Also exempt are certain medical or counsellor records relating to both pupils and members of staff.

14 Data security and Accountability

14.1 The School takes the responsibility for complying with the GDPR at the highest management level, with the Governors and throughout the organisation and will process all personal data that it holds in accordance with this policy.

14.2 The School will take a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;

- having written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures highlighted here and below such as entry controls with any stranger seen in entry-controlled areas being reported and secure lockable desks and cupboards with desks and cupboards kept locked if they hold confidential information of any kind (personal information is always considered confidential);
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection audits for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer who will bethe Bursar and Clerk of the Governors- Ian Findlay and
- adhering to relevant codes of conduct and signing up to certification schemes
- We review and update our accountability measures at appropriate intervals.

14.3 The School will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if the data processor agrees to comply with those procedures and policies, or if they put in place adequate measures.

14.4 The School will maintain data security by protecting the confidentiality, integrity and availability of the personal data, as follows:

- **confidentiality** means that only people who are authorised to use the data can access it;
- **integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;
- **availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the School's central computer system instead of individual PCs.
- **methods of disposal -** paper documents should be shredded and digital storage devices should be physically destroyed when they are no longer required;
- **equipment -** data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

15 Breach notification of Personal data breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the School becoming aware of it and may be reported in more than one instalment. Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. If the breach is sufficient to warrant notification to the public, the School will do so without undue delay.

16 Exemptions

16.1 Certain data is exempted from the provisions of the GDPR in the following situations:

- the prevention or detection of crime;
- the assessment of any tax or duty; and
- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

16.2 The above are examples of some of the exemptions under the GDPR. Any further information on exemptions should be sought from the DPC.

17 Enforcement

17.1 If an employee believes that the School has not complied with this policy or acted otherwise than in accordance with the GDPR, the employee should use the Grievance Procedure and should also notify the DPC.

Reviewed by Lupton Fawcett, May 2018

Appendix 1

Subject access request form

Please read the following prior to making your request –

Subject to certain exemptions, you have the right to ask whether any personal data is held about you, how we use this data and how it is processed. You also have a right to a copy of that information in a permanent form except where the supply of a copy is not possible or would involve disproportionate effort, or if you agree otherwise. The School will only release that personal information once it is satisfied as to your identity.

If the release of the personal information will disclose information relating to another individual(s) who can be identified from that information the School is not obliged to comply with the request unless:-

- The other individual has consented to the disclosure of personal information
- It is reasonable in the circumstances to comply with the request without the consent of the other individual(s)

Bradford Grammar School may deny access to information where the Data Protection GDPR allows. We will endeavour to provide you with requested information within one month. We can impose a charge for this information if the request is manifestly unfounded or excessive. If we do refuse a request, we will advise you accordingly within one month. If this eventuality did arise you have the right to complain. In addition, without prejudice you have the right to lodge a complaint direct to the Information Commissioner's Office if you have any concerns in relation to our information rights practices. The details are listed below for your information:
https://ico.org.uk/concerns/
ICO Helpline – 0303 123 1113

To the Data Protection Controller

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records*

	• *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Declaration

To be completed by all applicants *By signing below, I confirm that I am the data subject named above, or an authorised representative and that you can contact me if necessary if you wish to obtain further identifying information before agreeing to the request.* *I acknowledge that you may also need to contact me to obtain any further information that you require to enable you to comply with my request.*	
Signed:	*Date:*
Warning: a person who impersonates or attempts to impersonate another may be guilty of a criminal offence.	