# Bury Grammar Schools Data Protection Policy

**Policy agreed:** May 2018

**Policy Review Date:** April 2020

## Introduction

Everyone has rights over the way their personal data is collected and used. As a School, we collect, use and store personal data about our current, past and prospective: pupils and staff, parents/guardians, supporters, governors, alumni, suppliers and other third parties. We recognise that the correct and lawful treatment of this personal data will maintain confidence in the School and will provide for a successful working environment for all.

Please take the time to read this Policy as it sets out what information we collect about you, how we use it and how we keep it safe. By applying to or contracting with the School or providing information to us, you agree to its terms.

## About this Policy

"We", "our" or "us" means The Bury Grammar Schools Trustee Limited (company number 06612259) as trustee of Bury Grammar Schools Charity (registered charity number 526622). Our registered office is: Farraday House, Bridge Road, Bury, BL9 0HG.

The types of personal data that we may handle includes information about our current, past and prospective pupils, parents/guardians, staff members, donors, governors, alumni, suppliers and other third parties. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 incorporating the General Data Protection Regulation (the “Act”) and other legal requirements.

This policy (and any other policies or documents referred to in it) sets out the basis on which we will collect and use any personal data we collect from individuals, or that is provided to us by individuals or other sources and sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, use, transfer and store personal data.

All members of staff with access to personal data are obliged to comply with this policy.

The School has appointed a several Data Protection Champions each of whom ensure that their area is compliant with the Act and with this policy. The School has also appointed a Data Protection Central Contact who will pass any correspondence relating to Data Protection to the relevant Data Protection Champion. To contact the Data Protection Central Contact please

email dataprotection@burygrammar.com. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Central Contact.

**Other Relevant Policies**

This policy is intended to provide information about how the School will use (or "process") personal data.

This information is provided in accordance with the rights of individuals under data protection law to understand how their data is used. Staff, governors, parents and pupils are all encouraged to read this policy and understand the School's obligations to its entire community.

This policy applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This policy also applies in addition to the School's other relevant terms and conditions and policies, including:

- any contract between the School and its staff or the parents of pupils;
- the School's policy on taking, storing and using images of children;
- the School's CCTV Policy;
- the School's Data Retention Policy and Privacy Policies;
- the School's safeguarding, pastoral, and health and safety policies; and
- the School's policies, including its Acceptable Use Policy, E-safety Policy, Remote Working Policy and IT Security Policy.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should also be aware of and comply with this data protection policy, which also provides further information about how personal data about those individuals will be used.

The following policies are referred to in this policy and must be read and complied with so that we are complying with our data protection obligations:

Data Retention Policy;

Data Protection Rights of Individuals Policy and Procedure;

Data Breach Policy and Data Breach Notification Procedure

Employee Handbook;

**Data Protection Principles**

Anyone processing personal data must comply with the following principles. Personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and, kept up to date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed; 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.

**Lawful Processing**

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, it must be on the basis of one of the legal grounds set out in the Act:

- the data subject has given consent;
- processing is necessary to perform a contract to which the data subject is party or in order to take steps at the data subject's request before entering into a contract;
- processing is necessary to comply with a legal obligation;
- processing is necessary to protect the data subject's or another person's vital interests;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- processing is necessary for the controller's or a third party's legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

When **special categories** of (or sensitive) personal data are being processed, additional conditions must be met:

- the data subject has given explicit consent;

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the data subject's or another person's vital interests where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of it's legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- processing relates to personal data which has been manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health; and
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

**Processing for specific purposes**

In the course of our activities, we may collect and process the personal data set out in *0*. We will only process personal data for the specific purposes set out in *0* or for any other purposes specifically permitted by the Act.

**Transparent processing**

Where we collect personal data directly from data subjects, we will inform them about:

- our identity and contact details;
- the contact details of Data Protection Central Contact
- the purposes of the processing we are carrying out and our legal basis for processing;
- where we are relying on our legitimate interests as the legal basis for processing, what those legitimate interests are;
- the recipients or categories of recipients of the personal data;
- if applicable, that we may transfer personal data to a country or organisation outside the UK/EEA and the safeguards we have in place to protect the personal data being transferred;
- how long we will keep the personal data, or if that is not possible, the criteria used to determine that period;

- the data subject's right to have access to and correction or erasure of personal data or restriction of processing or to object to processing as well as the right to data portability;
- where the processing is consent, the existence of the right to withdraw consent at any time;
- the right to complain to the Information Commissioner's Office ("ICO");
- if the individual is required to provide personal data for statutory or contractual reasons, or because it is necessary to enter into a contract, and of the possible consequences of failure to provide personal data; and
- the existence of any automated decision-making, including profiling.

If we receive personal data about a data subject from other sources, we will provide the data subject with appropriate information to comply with the Act as soon as possible after we have received it.

**Adequate, relevant and non-excessive processing**

We will only collect personal data to the extent that it is required for the specific purpose(s) notified to the data subject.

**Accurate personal data**

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

**Only kept for as long as we need it**

We will not keep personal data longer than is necessary for the purpose or purposes for which we collected it. Personal data will be retained, and then securely destroyed, in line with our Data Retention Policy.

**Processing in line with data subjects' rights**

We will process all personal data in line with data subjects' rights, in particular their right to:

- request access to any personal data we hold about them;
- have any inaccurate personal data we hold about them corrected;
- be forgotten;
- restriction of processing, including preventing the processing of their personal data for direct marketing purposes;
- object to processing, including objecting to our legitimate interests;
- data portability; and
- withdraw consent.

We will ensure that we allow data subjects to exercise their rights in accordance with our Data Protection Rights of Individuals Policy.

**Data security**

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Personal data will only be transferred to a processor if we are satisfied that they have adequate data protection policies and clauses in the contact with the School.

We will maintain data security by protecting the confidentiality, integrity, availability and resilience of the systems we use to process personal data, defined as follows:

Confidentiality means that only people who are authorised to use the personal data will be allowed to access it and we will not disclose personal data to anyone who is not entitled to and only when they enter into appropriate confidentiality undertakings.

Integrity means that measures will be used to protect any processing or storage of personal data from unauthorised or unlawful access or from loss or destruction.

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 our central computer system instead of individual's laptops or PCs.

Resilience means that we will have procedures in place to restore the availability of and access to personal data in a timely manner in the event of any incidents.

Our security procedures are set out in detail in our IT Security Policy. In summary, our security procedures include:

Password protection. Staff members will set up passwords to access our systems and documents and will ensure that their passwords are kept confidential.

Access controls. Certain areas of our system and certain documents will only be accessible by the members of staff who have sufficient authority to access them.

Firewalls and antivirus. We use appropriate firewall and antivirus products on our computer systems to ensure their security and integrity. We test and update these products as necessary to ensure they are adequate.

Encryption and 2 factor authentication. We use encryption and 2 factor authentication on our systems and devices when appropriate and where possible.

Equipment and screen locks. 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. Any other devices that have personal data on them (such as laptops and tablets) must have screen locks and the data users must ensure that they lock the screens when not using the devices.

Removable hardware. In the event that any removable hardware is used (for example USB or memory sticks), this should be password protected and encrypted to ensure that there is no unauthorised access to the personal data on it.

Paper documentation. No paper documentation containing personal data is to be left out when not being used and hard copies of electronic copies of personal data should not be made unless needed.

Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind, including personal data which is always considered confidential.

Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

We will ensure that we allow data subjects to exercise their rights in accordance with our Data Protection Rights of Individuals Policy.

**Marketing and consent, keeping in touch and supporting the school**

The School will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the school, alumni and parent events of interest, including by sending updates and newsletters, by email, telephone, SMS and by post. Unless the relevant individual objects, the school may also share personal data about parents, pupils and alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community. Consent will be obtained to pass information to The Old Girls Association and the Old Boys Association and also for publicity in external media.

The School may contact parents and/or alumni (including via the organisations above) by post, email, SMS and telephone, and email in order to promote and raise funds for the school;

Where we carry out any of the above communications, we ensure that this is only done in a legally compliant manner based on consent or on the legitimate interests of the School when appropriate.

We will also ask parents if they are happy for their child's photographs to be used by us, for example on our website or in our publications. Where we use pupils' photographs, we ensure that this is only done in a legally compliant manner based on consent.

When we use photographs of pupil, parents, alumni and supporters in media publications we will gain consent from the individual or the parent of pupils under the age of 13 prior to publication.

We will ensure that individuals are aware that they can withdraw consent at any time, and will communicate with them how they can do so, for example we have unsubscribe links on our email communications and we ensure that pupils are told they can withdraw consent to having their photographs used by contacting us in writing.

We will record consent accurately and will ensure that we contact individuals every four years to update individual details make sure that they are still happy to receive marketing communications from us. If we receive any withdrawals of consent, we will action these as soon as possible and record that the individual no longer wishes to receive marketing communications from us, or does not wish to have their photograph used.

**Automatic processing**

We monitor the activities of data users who use School devices. This is explained in more detail in the Employee Handbook and in the IT Security Policy.

We also monitor the behaviour of users of our website using Google Analytics. This is explained in more detail in *0* and in our Website Users Privacy Policy.

We also use biometric data readers in our canteen tills to identify pupils and staff members. This is explained in more detail in our Biometric Policy.

We do not make any decisions about individuals that would produce legal (or similar) effects based solely on automated processing.

**Transferring personal data to a country outside the EEA**

If we transfer any personal data we hold to a country outside the European Economic Area, we will ensure that one of the following conditions applies:

- the EU Commission has made an adequacy decision about that country; or
- if there is no adequacy decision, we have in place:
    - a legally binding and enforceable instrument between public authorities;
    - binding corporate rules;
    - standard data protection clauses adopted by the EU Commission;
    - standard data protection clauses adopted by the ICO and approved by the EU Commission;
    - an approved code of conduct together with binding and enforceable commitments to apply the appropriate safeguards; or
    - an approved certification mechanism together with binding and enforceable commitments to apply the appropriate safeguards.

**Disclosure and sharing of personal information**

Occasionally, the School will need to share personal information relating to its community with third parties, such as professional advisers (lawyers, accountants, pension providers etc) or relevant authorities (HMRC, police or the local authority or other Government Department etc).

For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records held and accessed only by authorised School staff, or otherwise in accordance with express consent; and
- pastoral or safeguarding files.

However, a certain amount of any SEN pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires. In addition certain medical information necessary to keep pupils safe whilst in our

care e.g. pupils with severe allergies, and certain ongoing medical conditions that require regular medication e.g. diabetes, will be shared with staff on a need to know basis in the context of health and safety.

Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including Keeping Children Safe In Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the Lado or police. For further information about this, please view the School's Safeguarding Policy.

In accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems and software, web development and/or cloud storage provision. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

We may also disclose personal data we hold to third parties:

- if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation;
- in order to enforce or apply any contract with the data subject or other agreements;
- to protect our rights, property, or the safety of our employees, pupils, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We may also share personal data we hold with the selected third party processors.

**Changes to this policy**

We reserve the right to change this policy at any time and may need to do so to ensure the effective running of the School. Whenever we make any significant changes to this policy, we will post a revised version on our website and notify parents, pupils, staff, governors, alumni and other members of the School's community that we have done so.

## Schedule 1

### Data Processing

In order to carry out our ordinary duties to staff, pupils and parents, the School may process a wide range of personal data about individuals including current, past and prospective: staff, pupils, parents/guardians, governors and contractors as well as supporters as part of its daily operation.

The school will need to carry out some data processing regarding individuals in order to fulfil its legal rights, duties or obligations, including those under a contract with its staff, contractors or parents/guardians of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The School expects that the following uses may fall within that category of its (or its community's) "**legitimate interests**":

- For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);
- For the purposes of administering bursaries in accordance with the School's Bursary Policy;
- For the purposes of collecting school fees;
- To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils, UCAS provision and monitoring pupils' progress and educational needs;
- Maintaining relationships with alumni and the School community;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- To safeguard pupils' welfare and provide appropriate pastoral care including emergency contacts;
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT Acceptable Use Policy (Staff and Pupils) and IT Security Policy;

- To make use of photographic images of staff and pupils in School publications, on the School website and (where appropriate) on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- For the purposes of staff/employee selection and for all aspects relating to the employment of staff
- For the purposes of selecting and the ongoing management of Governors
- For the purposes of vetting and entering into a contract with all External Providers and Hirers of the School's facilities
- For the Health and Safety and Security of all employees, pupils, contractors and visitors to the School
- For the purposes of carrying out a contract with a supplier
- For security purposes, including CCTV in accordance with the School's CCTV policy; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

In addition, the School may need to process **special category personal data** (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so: for example for medical advice, social services, insurance purposes or to organisers of School trips;
- To provide educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- In connection with employment of its staff, for example DBS checks, welfare or pension plans;
- To run any of its systems that operate on biometric data, such as for security and other forms of staff and pupil identification (e.g. lunch); or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

**Types of personal data processed by the school**

This will include by way of example:

- Names, addresses, telephone numbers, e-mail addresses and other contact details;
- Car details (about those who use our car parking facilities);
- Biometric information, which will be collected and used by the School in accordance with the School's Biometrics Policy.
- Bank details and other financial information, e.g. about parents/guardians who pay fees to the School and those who apply for the School's Bursary Scheme and supporters of the School, staff;

- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks', ID;
- Where appropriate, information about individuals' health, and contact details for their next of kin;
- References given or received by the School about: past, current and prospective staff, governors, contractors and pupils, and information provided by previous educational establishments and/or other professionals or organisations working with staff, contractors and pupils ; and
- Images of pupils, staff, visitors, contractors, alumni (and occasionally other individuals) engaging in School activities, and images captured by the School's CCTV system (in accordance with the School's policy on taking, storing and using images of children).