Data Protection Policy

Date Approved: April 2020
Last reviewed: September 2023
Review Date: September 2025
Author: R Berry
This policy is for Bury Grammar School

1. Background

Data protection is an important legal compliance issue for the School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's privacy notices). The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (**GDPR**) – an EU Regulation that is directly effective in the UK, regardless of Brexit status – and a new Data Protection Act 2018 (DPA 2018) was also passed to deal with certain issues left for national law. The DPA 2018 included specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. Definitions

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or 'personal data'):** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. Application of this policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

4. Person responsible for Data Protection at the School

The School has appointed Mrs C Lynskey (Director of Communications) and Mr R Berry (Finance Director) as Data Protection Champions who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. 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 Data Protection Central Contact who will pass correspondence to the relevant Data Protection Champion. The Data Protection Central Contact can be emailed at: dataprotection@burygrammar.com.

5. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;

4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the

personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the employee handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with School' Safeguarding and Acceptable Use Policies. In addition, there are a number of data related policies, procedures and guidance notes within the staff handbook, for which all staff are required to read and comply with. Examples of such polices include:

- *Biometric Policy*
- *Remote Working Policy*
- *Data Breach Notification Policy*
- *Data Retention Policy*
- *Photography and Videoing Policy*
- *IT and Information Security Policy*

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

A key GDPR obligation is reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify one of the data champions immediately. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to one of the data champions, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

8. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell one of the data champions as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and

  withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell one of the data champions as soon as possible.

9. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We must 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 or give access to personal data to anyone who is not entitled to do so 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. Where appropriate, personal data should therefore be stored on our central computer system instead of an individual's laptop or PC.

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. Members of staff 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 the authority and need 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. Members of staff must ensure that individual monitors, laptops or other devices do not show confidential information to passers-by and that they lock their screen or log off from their device when it is left unattended.

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. Where a worker or member of staff is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.

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. Any member of staff who removes data from the School, whether in paper or electronic form must adhere to all the School's GDPR procedures and policies.

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

Third parties. No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.

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

10. Marketing

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 must 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 must 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 must 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 members of staff must gain consent from the individual or the parent of pupils under the age of 13 prior to publication.

Members of staff must ensure that individuals are aware that they can withdraw consent at any time, and communicate with them on how they can do so, for example we should have unsubscribe links on School email communications and we let pupils know that they can withdraw consent to having their photographs used by contacting us in writing.

When consent is given it must be recorded by staff accurately and we should contact individuals at least every four years to update individual details and make sure that they are still happy to receive marketing communications from us. If we receive any withdrawals of consent, staff must 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.

11. Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Finance Director. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance

numbers or passport details), may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

SUMMARY

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School’s culture and all its staff and representatives need to be mindful of it.

Data Protection Policy Issues and Updates

Date	Policy version	Summary of key change(s)
September 2023	1	Change of named data protection champions